Joint Economic Committee Hearing

Economic Espionage, Technology Transfers and National Security

Tuesday, June 17, 1997

Witnesses:

Lieutenant General Robert L. Schweitzer, U.S. Army (Retired)
Expert on Weapons Proliferation.

Dr. Peter M. Leitner
Author of "Decontrolling Strategic Technology, 1990-1992."

Mr. John J. Fialka
***Wall Street Journal* Reporter and Author of "War By Other Means."**

Dr. Kenneth Flamm
Author of "Mismanaged Trade? Strategic Policy and the Semiconductor Industry."

Chairman Jim Saxton's Prepared Statement

Retired Lt. Gen. Robert L. Schweitzer's Prepared Statement

Dr. Peter M. Leitner's Prepared Statement

Mr. John J. Fialka's Prepared Statement

Dr. Kenneth Flamm's Prepared Statement

Return Home

Statement of Chairman Jim Saxton
Joint Economic Committee
June 17, 1997

Economic Espionage, Technology Transfers and National Security

Ladies and gentleman, good morning. Thank you all for being here.

The Joint Economic Committee sits in a very unique position and I would suggest an ideal position to evaluate past policy and to evaluate those policies' impact on our economy, particularly, in the context of the legislative intent of the authors of the policies.

The areas of concern that I have learned of occurred across several administrations in both the areas of high technology transfer and economic espionage. My goal is to shed light on these problems.

I am sure that those responsible for these policies formulated them with the best of intentions. However, those intentions may not have manifested themselves as expected in this new and changing reality of a former Soviet Union, an emerging Asia and a struggling, unstable Third World.

I am pleased to welcome to the committee an extremely knowledgeable group of panelists.

Dr. Peter Leitner is the author of a new book entitled "Decontrolling Technology: Creating the Military Threat for the 21st Century." I would like to make it clear that Dr. Leitner will testify as the author of that book and not in his official capacity as a Foreign Trade Advisor for the Department of Defense. Additionally, Dr. Leitner is the author of the book "Law of the Sea Treaty" which also highlights concerns about mandated high technology transfer. Dr. Leitner's professional background also

includes serving as a senior licensing officer for U.S. exports to various proscribed countries including China, Libya, Iraq, former Warsaw Pact countries, Iran, and India. Dr. Leitner is currently DoD's representative to the interagency Subcommittee on Nuclear Export Controls.

Our second panelist is Lt. Gen. Robert Schweitzer (Ret). General Schweitzer retired from the United States Army after 36 years of service with assignments including: Director of Strategy, Plans and Policy; Deputy Chief of Staff for Operations and Plans; National Security Defense Group Director; and the Chief of the Policy Branch of SHAPE in Belgium. General Schweitzer has received numerous awards and decorations including the Army Distinguished Service Cross, the Defense Distinguished Service Medal, the Army Distinguished Service Medal, three Silver Stars, two Defense Superior Service Medal, two Legion of Merits, the Distinguished Flying Cross, the Soldiers Medal, the Bronze Star with Valor device (three additional awards), Air Medal with Valor device (20 additional awards), seven Purple Hearts, and two Army Commendation Medals.

General Schweitzer will testify today about the proliferation of a devastating new weapon developed by the former Soviet Union and is currently in enhanced development today in Russia, with previous systems being sold by Russia. The weapon is the Radio Frequency Weapon on Electromagnetic Pulse weapon used, among other things to cripple computer capability. It has only been in the last few weeks that the information has been declassified about EMI. Previously, only those with the highest security clearance even knew about this weapon system in any detail.

Our third panelist is Mr. John Fialka. Mr. Fialka is a well-known and respected reporter for the **Wall Street Journal**. Mr. Fialka is the author of "War by Other Means," an important but disturbing book on high tech transfer and Foreign Intelligence Services conducting espionage in the United States. After a brief stint at the National Petroleum Refiners Association, Mr. Fialka began his journalism career at the Baltimore Sun and then moved on to the **Washington Star**. In 1981, Mr. Fialka moved to the **Wall Street Journal** and has worked both in the London bureau and in his current position in Washington. Mr. Fialka has been awarded numerous honors from such organizations as the American Bar Association, the National Science Writers Association, the National Headliner, and Worth Bingham. Additionally, Mr. Fialka is the author of the book "Hotel Warriors" which is an analysis of the press coverage of the Persian Gulf War.

Our final panelist is Kennneth Flamm. Mr. Flamm has been a Senior Fellow in

the Foreign Policy Studies program at the Brookings Institute since 1995, a position he also held from 1987 to 1993. From 1993 to 1995, Mr. Flamm served as Principal Deputy Assistant Secretary of Defense for Economic Security and Special Assistant to the Deputy Secretary of Defense fro Dual Use technology Policy. At Brookings, Mr. Flamm has focused much of his research on international competition in high technology industries.

Let me add on final note. The people of our country owe a collective debt of gratitude to the men and women who serve this country in our law enforcement and intelligence services, and especially those dedicated Asian Americans without which the security of this country could not be guaranteed. Over 20 countries conduct espionage against the United States. Let me make it perfectly clear that the criminal actions of a few do not reflect the character, honesty, and loyalty of ethnic Americans - without whom these spies would not be apprehended.

I look forward to the enlightening testimony of each of our panelists.

Return Home

Statement by

Lieutenant General Robert L. Schweitzer
U.S. Army (Retired)

before the

Joint Economic Committee
United States Congress

June 17, 1997

Radio Frequency Weapons and the Infrastructure

I have been asked to talk to the overall subject of your hearing from a somewhat different perspective. Initially, it was to be from the one of what technology transfer means to a soldier. That part would have been fairly simple to address. Field soldiers are too busy to think much, if at all, about such transfers. That is, until they run across them on a battlefield where U.S. technology or materiel is being used against them. That happened in World War II when the residue of simpler technologies in the form of scrap metal was employed against us in the Pacific. It happened in Vietnam when some of our weaponry was obtained by our adversary. It happened again in Desert Storm when we ran across containers of U.S. materiel in the hands of Saddam Hussein's soldiers, materiel which had been channeled through Jordan. Then the fleeting reaction is one of anger and "why?" But soldiers--placed as they are since the time of the Roman legions in the sand, mud, rain and snow to fight decisive battles--are really too busy to brood much about such things. They are, however, grateful when Congress acts ahead of time to bar technology transfers, not only the simple ones of which I speak but the more serious, albeit subtle ones, which can affect the outcome of battles and wars.

Today there is a new class of radically new and important radio frequency weapons (RFW) which merits your attention as it emerges. And in this case, the horse is out of the barn. Transfers have occurred and are occurring. Equally true, however,

is the fact that there are things that can be done to protect our nation, which is the underlying objective of today's hearing. Certainly one of these things is to recognize that export control documents, particularly the Militarily Critical Technologies List, needs to be reviewed to determine if radio frequency technologies should be considered in the same careful way we do nuclear technologies. I respectfully suggest that this is the case; stronger controls are needed. One example is Reltron tubes which went to a friendly nation, one who sells products widely--sometimes to nations who do not like us. These tubes, which can be small or large, generate intense radio frequency pulses and can be used as RF weapons.

Before we go further I wish to state clearly for you and for the public record that I do not speak for the Department of Defense, for any military service or any government agency. I come before you only as one who has researched this area for the past year and is writing a White Paper on the subject, one which will be offered to DoD for their use and disposition.

Some of you may know about radio frequency weapons, where they came from, what they can do and what the implications are.

Although there are a number of groups and individuals concerned with this subject, I have found that somewhat paradoxically the word has not really gotten out in Washington itself. Despite the existence of a Presidential commission, an Infrastructure Protection Task Force, a Critical Infrastructure Working Group, an Information Warfare School at the National Defense University, and other working groups, to include divisions on the Joint Staff in the Pentagon, as well as a few very dedicated and brilliant mid-level people in DoD, a general understanding is lacking. This is true not only of RFW, but of their immediate threat to our DoD and national infrastructure. Indeed the term "infrastructure" is so amorphous that it lacks impact if not meaning. One of our first tasks will be to define what is the military and economic infrastructure and what in it is susceptible and vulnerable to RF weapons.

Some 90 to 100 references in 26 pages of the 70-page Quadrennial Defense Review speak to this new threat, but only to a discerning reader; the name for the class is not used. On the other hand, a recent search of the Internet found 2,400 to 2,800 references, while yet another, more thorough search found many tens of thousands of documents where the key words "radio frequency weapons" appear. Some very good people have written books and articles on the subject, the first revealing article known to me appeared in 1987 in the Atlantic Monthly, but for many reasons the knowledge is diffused. In the public sector the subject has yet to draw any

real attention or concerted action.

To help set the stage, recognize with experts like a former NSA Director that we are the most vulnerable nation on earth to electronic warfare. This thought is echoed by a former CIA Deputy Director, and a former Deputy Attorney General who forecast that we will have an electronic Pearl Harbor if we do not accept a wake up call. Our vulnerability arises from the fact that we are the most advanced nation electronically and the greatest user of electricity in the world.

On the military side, as in the civilian sector, our current superiority is based on microelectronics. To prevail against us, an adversary must cripple, destroy or deny access to those same microelectronics. Can an adversary do so? Very likely, as this hearing will bring out. All of our military doctrine assumes extensive use of sophisticated electronics and communication systems to ensure information dominance and overwhelming battlefield success. As is the case with our civilian infrastructure and economy, our current dependence is large and will continue to grow. Because our battlefield success and the well being of our civilian economy--with which this committee is especially charged–-are so dependent upon the effectiveness of our microelectronic-based systems, we should fully understand any technology that might be used to defeat our systems. This is particularly true of the newly emerging threat of radio frequency weapons. And even more importantly, we must develop countermeasures before such weapons are used against us.

Before going further, let me explain what these weapons are, where the Russian work has gone since 1949 and the applications of these weapons. If you are interested--as I believe you will be--you may wish to bring before you successive panels of our own leading scientists and experts. I have talked to many of them, heard them make presentations at conferences, and read their articles and books. I will be pleased to provide your staff with names of those who could provide this or other committees with a better understanding. I am also willing to assist in any way that might be helpful.

First of all, an RF weapon is one that uses intense pulses of RF energy to destroy ("burnout") or degrade ("upset") the electronics in a target. These weapons can be employed on a narrow beam over a long distance to a point target. They are also able to cover broad targets. They are categorized as high power microwave (HPM) weapons and ultra wide band (UWB) weapons.

The phrase non-nuclear electromagnetic pulse is sometimes used, because these

weapons, which are indeed non-nuclear, project the same type of pulse we first learned of in conjunction with nuclear weapons. As a practical matter, a piece of electronic gear on the ground, in a vehicle, ship or plane does not really care whether it is hit by a nuclear magnetic pulse or a non-nuclear one. The effect is the same. It burns out the electronics. The same is true of the computers in this Senate office building, in industry, or on Wall Street.

There is another way these weapons can be delivered to a target, military or civilian. Here the term RF munitions, or RFM is used. Yet these too are properly called RF weapons. These small munitions contain high explosives that produce radio frequency energy as their primary kill mechanism. In the hands of the skilled Russian scientists, these munitions come as hand grenades, mortar rounds, or large artillery shells or missiles. Generally, they produce a short but very intense pulse. While not yet fully understood and with some uncertainties argued as to their capabilities, many scientists are convinced the weapons actually exist. Without making any claims as to what they can do, I offer the following list from open source FSU literature of some nine smaller RF munitions or weapons:

- **Magnetohydrodynamic Generator Frequency (MHDGF)**
- **Explosive Magnetic Generator of Frequency (EMGF)**
- **Implosive Magnetic Generator of Frequency (IMGF)**
- **Cylindrical Shock Wave Source (CSWS)**
- **Spherical Shock Wave Source (SSWS)**
- **Ferromagnetic Generator of Frequency (FMGF)**
- **Superconductive Former of Magnetic Field Shock Wave (SFMFSW)**
- **Piezoelectric Generator of Frequency (PEGF)**
- **Superconducting Ring Burst Generator (SCRBG)**

Some of these weapons are said by the Russians to be now available as a hand grenade, a briefcase-like object, a mortar or artillery round.

Applications or potential targets (like those of the larger High Power Microwave weapons) would include all military computers, circuit boards, or chips, of any description, and include the following key components of our military and national infrastructure. They would have equal impact on civilian targets with the advantage less power would be required. Recall that the term "infrastructure" lacks clear meaning, but would include things like:

- The national telecommunications systems

- The national power grid
- The national transportation system, to include especially the FAA but also such simple things as our traffic lights (with consequent gridlock)
- The mass media
- Oil and gas control and refining
- Manufacturing processing, inventory control, shipment and tracking
- Public works
- Civil emergency service
- Finance and banking systems (to include bank's ability to dispense cash)

This list of potentially vulnerable targets could and should be extended to include airplanes, ships, vehicles and the like. Of interest is the fact that we are doubly vulnerable because we are, and will remain, in an era of dual use of military and civilian systems. For example, 90% of our military communications now passes over public networks. If an electromagnetic pulse takes out the telephone systems, we are in deep double trouble because our military and non-military nets are virtually inseparable. It is almost equally impossible to distinguish between the U.S. national telecommunications network and the global one. What this means is that it is finally becoming possible to do what Sun Tzu wrote about 2000 years ago: to conquer an enemy without fighting. The paradigm of war may well be changing. If you can take out the civilian economic infrastructure of a nation, then that nation in addition to not being able to function internally cannot deploy its military by air or sea, or supply them with any real effectiveness--if at all.

Since 1949, the intense interest of the former Soviet Union in developing these weapons appears to have resulted from their recognition that they could not match the capability of Western electronics, and their belief that RFW have the potential to be effective against our sophisticated electronics. It is far less clear to me and to others why they are willing to transfer and proliferate the RF technologies they have developed so carefully and so well, but that they are clearly doing so. Should you wish, a future hearing by this or another committee could go into more detail.

President Yeltsin proposed to President Clinton a joint program for a "plasmoid defense" against ICBM's. While it is unclear to many scientists what President Yeltsin meant, such a defense, if attainable, might presumably set up a shield which would ionize the atmosphere and cause missiles to fail. Official Russian journals and publications show keen interest and provide many details about these weapons. A great amount of information is flowing continuously from three former Soviet Republics on their past and current programs.

We do know that the reduction in military spending by the FSU and many Western nations is prompting the defense industries of many countries to offer advanced weaponry to foreign customers to further their own research, development and industrial capabilities. This trend is almost certain to grow over the next 10 years.

From unclassified sources, we know that Russia, Ukraine, the United Kingdom, China, Australia and France are well ahead in this field, while Germany, Sweden, South Korea, Taiwan and Israel are emerging and have ample details of the Russian work and of the proceedings of more than 20 years of international conferences. Without going into any classified matters one may reasonably infer that the pariah nations have similar interests and some certainly have the financial resources to develop or procure RF weapons.

Russian and FSU information on RFW has been moving across borders for many years. International conferences beginning in 1949 have been a principal source of technology transfer. Scientists here and abroad have long exchanged papers, letters and, with increasing frequency, telephone calls.

- The first Megagaussing Conference on the generation of high power electromagnetic pulses took place in 1949 in Frascati, Italy. Russian scientists were key players in what has become a long series of presentations on the generation of electromagnetic power. Present at this and many subsequent conferences was the U.S. inventor of RF weapons, Dr. Max Fowler. His picture was placed over the center of the Moscow desk of one of his Russian counterparts who is a leader in the Russian development of the smaller version of these weapons. The latter is a key figure in the offer to sell RFW and RFM or their technologies to others.

- EUROEM Conferences have been meeting (with name changes) for perhaps some 20 years at about two-year intervals. At the 1994 conference which was held in Bordeaux, France, the Russians made public many details of their long work in these weapons. Some of their papers deal with the strategy, tactics and techniques for the use of offensive RF weapons. Among nations participating were Iran and Iraq. At this conference the Russians talked about selling their technology and weapons to prospective buyers. I am told that subsequently a large number of nations have engaged them in some form of negotiations. Some of these "buyers" raise legitimate concerns.

- The BEAMS conference (with name changes) has been meeting about every two years since 1975.

- The EUROEM Conference met in Albuquerque in 1996; the BEAMS Conference met that same year, I believe in Prague. Attendance was open to all nations.

- The next EUROEM and BEAMS conferences will meet in 1998 in the Middle East, two weeks apart in Tel Aviv and Haifa, respectively.

- An International Pulse Power Conference held their tenth conference under that name in 1995, but has existed under other names for a longer period of time.

- The International Particle Accelerator Conference has also met for more than 20 years.

- The American Physical Society has a Plasma Physics Division which hosted (for more than 20 years) many conferences. Usually each one has several sessions on microwave generation.

- And there are more. . .

Understanding the number, frequency and long standing nature of these conferences, you can perhaps better appreciate why I earlier said that the horse is out of the barn. Of interest, too, is the role of the United States in these conferences. Indisputably, the U.S. is the scientific powerhouse of the world. We have initiated and hosted a number of these conferences, funded many of them to a significant degree, and played a prominent role at all. While we gain some information, our scientists will readily acknowledge the net advantage is always to other attendees.

Put another way, from a narrow technology transfer standpoint we have thus far lost more than we gained. However, even prior to the Internet no one could control the flow of ideas, especially among scientists. They like to talk especially about what they have achieved, and how they solve theoretical and practical problems. For decades our scientists have found their Russian counterparts to be brilliant, dedicated and creative. Personal relations are important and some have developed, but they are exceptional. For the most part the Russians have been ambiguous about their great

work and often are mistrustful of Americans. We should move to change that by closer and warmer contacts as well as by efforts to enter into joint ventures--with all the travails that accompany such efforts. The Russians are intensely interested in our comments and some professional appreciation by their scientific peers of their decades of work on the offensive use of RF weapons. In my humble opinion they would prefer to work with our own distinguished scientists rather than others, but will sell their technology and products to others. I believe there is a real potential for joint ventures which could serve to constrain to some degree the proliferation of these weapons, especially to those who would do us harm.

To return to the earlier point about the need for better controls of technology transfer, consider these two counterpoints which illustrate the problem:

- First: Although RF weapon components are on the Critical Technologies List, there are no up to date DoD guidelines or directives on this subject. An attempt to do so was made two years ago when little was known about the subject. As a consequence, decisions within the U.S. scientific community are becoming harder and dicier to make. There is a lack of clear policy guidance and direction.

- Second: The first point is illustrated by the transfer of the Reltron microwave tubes. These tubes, which generate radio frequency power, cost a great deal of money to produce and test. The U.S. is the leader in high-power tubes and their associated power systems, but the market is really thin. Our tube industry has no current buyers here in the U.S. Without major contracts from foreign countries (France, the United Kingdom, Germany and Israel, among others), our tube industry will die. We will lose contact with real customers and become dependent on foreign hardware for our systems. Ultimately we will increase the difficulties that must be overcome to develop HPM applications for any future DoD use. Almost certainly we would know less--almost nothing--about what was going on in this area. For their part the Europeans and others would not cease to procure; they would simply undertake their own development. So our high power microwave scientific community told the State Department on balance to approve the transfer, which State did. Inevitably one consequence will be to advance the work of others and ultimately the production of RF devices to be used wherever and however by whomever. Note well, however: there is no guarantee that friendly countries will not sell the devices they produce to unfriendly, even hateful people.

It would also appear that there are other proliferation and transfer concerns of interest to this committee, simply because there is so much accurate how-to-do information in the open literature and on the Internet. Several countries have RFW programs and Russia says it has sold some technologies to these countries. At least one of these countries has acknowledged such a transfer. The crux of the difficulty in controlling these transfers is best illustrated by the fact that High Power Microwave weapons look like ordinary radars. With a dish or horn antenna, and a van with a power source, an RFW would look like a new, used or renovated radar. Used ones are offered for sale today in military surplus and commercial catalogs. Other catalogs offer for sale the components to put together lower power, but also very low cost items, that once assembled could be used effectively against the infrastructure.

Users of the new weapons can be criminals, individuals or organized gangs of narco or domestic terrorists--or a determined, organized, well-funded foreign adversary, either a group or nation who hates us.

The Russians, as noted, led with this work starting in 1949 with theory. By 1961, they were doing research, as documented in their numerous unclassified scientific articles. Experiments began in the seventies and proceeded to testing as described in their publications. Many of these weapons appeared in written descriptions, some photographs and diagrams in the nineties. Strategy, doctrine, tactics and techniques are all laid out in rather clear form. Please note all of this is unclassified information.

There is a legitimate question about the intelligence aspect of all of this. Our intelligence community largely proceeds on the operating principle followed in the Cold War: A threat is not validated until it is fielded. Well and good; hard evidence is essential.

But the question may fairly be asked: does that principle serve us well in the present day? Suppose we were to take a Russian or FSU-designed weapon, fabricate it in the U.S. and test it here. If the results were to meet the standards of performance and capabilities now claimed by the Russians, would we then have a validated threat? The answer to the capabilities may be forthcoming this month because at an unclassified level one of our national labs is doing just that. Another lab has purchased cheap, off the shelf components and will test its lower power device this month. Their engineers and I believe it will indeed work against infrastructure and light military targets.

There is a great deal of other corroborating evidence which at least argues for the

existence--which is still disputed in some quarters--of these weapons: one minor one is an International Institute for the Prevention of Offensive RF Weapons, located in Philadelphia. Why such an institute if there are no such things? Evidence as to the capabilities of the weapons may be found in such recent statements as China's declared intention to purchase three RF weapons derived from the Russian technology. Another is the series of reliably reported discussions within the IRA of their intention to seek RF weapons for use against the London financial system in lieu of bombs and explosives. Consider, too, the recent statement by Sweden they have used these devices in experiments to stop cars at 100 yards, as well as their reported claim that RF weapons have been used against their financial institutions. A similar but much disputed statement has been reported by the London Times concerning British financial and banking institutions. The Los Angeles Police Department had done some successful work with vehicles in the interests of public safety and to halt fleeing suspects. Advantages of the larger high power microwave RF weapons include:

- Low cost per engagement
- All weather
- Instantaneous engagement times
- Simplified pointing and tracking
- Possible to engage multiple targets
- Deep magazines–simplified logistics (can "fire" or pulse as long as there is power in the generator)
- Non-lethal to humans when properly adjusted
- Well suited to covert operations because of lack of signature; deniability
- Not able to detect attacks; silent when used without explosive devices

The RFM offer many of the same advantages, offset only by the sound of the explosion that detonates them and produces the rise in pulse energy.

Unless we choose to be, we are not without courses of action. Some of these could be explored at a future hearing. Some preliminary thoughts are offered today:

- We either fully understand nor control this technology.
- We have not begun to work on defenses , especially for our vulnerable infrastructure.
- We need to first scope the problem, determine susceptibilities and vulnerabilities, then test.
- All of this, to include any appropriate hardening of existing components, will

take many years.
- There are other courses of corrective action, but all will take time to acquire and apply.
- The first step might well be to bring forward our real RF experts in DoD and the scientific community who know what needs to be done.

We need to go at this problem with a step-by-step sensible approach. No budget buster is proposed. Even if Congress had ready funds, a grandiose national solution is not the way to go.

We can start by scoping the problem and then by applying some of the same low-cost components that are now used in the ever expanding information technologies. Examples are surge-like protectors, plasma limiters, diodes, and metal covers. Parallel or redundant systems are another technique.

We are good at managing risks. We should no longer hesitate to reduce the impact of the threat, or to give our intelligence community the guidance to open up (some would say revise) their approach to this problem. Clearly the United States Congress will play a key role in whatever we do, or choose not to do, and our top leadership should focus on the longer term. But we should begin now in a sensible, modest way.

Three things we want to keep foremost in mind:

- Do not throw a lot of money at this problem. Funds don't exist; the best solutions will have to be devised.
- Do not tell DoD or the Services to take this out of their budgets. They are over stretched now and it would be wrong to tell them to pay for protection of the civilian infrastructure.
- Do not continue to do what we have been doing and ignore the problem.

Return Home

Statement by

Dr. Peter M. Leitner

before the

Joint Economic Committee
United States Congress

June 17, 1997

Feeding the Dragon: Technology Transfer and the Growing Chinese Threat

Mr. Chairman, members of the committee, I am the author of the book entitled *Decontrolling Strategic Technology 1990-1992: Creating the Strategic Threats of the 21st Century* published by University Press of America. I need to state up front that the opinions and analysis I express here are my own and do not represent the views of the Defense Department, the United States Government, or any other organization.

I am honored to appear before you today. I am quite pleased by the vision and concern that the chairman and committee members have shown regarding the long-term effects that technology acquisition by potential adversaries, particularly China, may have upon the military and economic security of the United States.

My motivation in writing this book stemmed from the dramatic politicization of the export control process. I have seen the blatant manipulation of honest technical and engineering analyses that warned of the dangers to U.S. national security posed by the proliferation of advanced dual-use technologies. Unfortunately, as I have documented, the campaign to weaken or eliminate the concept of "non-proliferation" by undermining the export control system -- its chief operational vehicle -- has been remarkably successful and can accurately be characterized as a scorched-earth policy. It has been so successful, in fact, that CoCom and the national security export controls that we came to know and rely upon no longer exist. In their place are a

handful of weak, ineffectual regimes which are little more than cardboard cut-outs designed to maintain the facade of an international technology security system but offer virtually no protection from nations seeking to develop advanced conventional weapons or weapons of mass destruction.

These so-called follow-on regimes are limited notification fora, similar in function to a post office box, where nations inform each other of denials of technology transfers if they so desire. The national discretion nature of decision making common to these regimes -- to include: Wassenaar, the Nuclear Suppliers Group, the Missile Technology Control Regime, and the Australia Group -- ensures that suppliers may do what they wish so long as some *post facto* notification is made to the partners. This *de minimis* approach is a far cry from CoCom's consensus-based regime where pre-notification was the rule and a negative vote cast by any of the 16 member states could actually prevent a dangerous transfer from taking place.

The current administration was responsible for the elimination of CoCom before any replacement regime was installed. The result was the loss of any possible negotiating leverage in ensuring that a follow-on regime would have any teeth. The so-called Wassenaar Agreement which was eventually formed is little more than a kabuki-like construct intended to provide the appearance of technology control while affording none. The unnecessary destruction of CoCom opened the floodgates of technology to China as it was subject to few restraints other than in the narrow realms of ballistic missile and nuclear technology. As the Chinese are already a nuclear and ballistic missile power the restraints serve only to place obstacles in front of Chinese acquisition of technology they already have while allowing the unrestricted flow of militarily important power projection and C4I technology that they need.

It is with these facts in mind that I focused on the relationship between the decontrol actions and the potential neutralization of billions of dollars this nation has invested in advanced technology -- stealth for example. I describe how, in a quest for a few hundred million dollars in potential sales, we have made available the means to offset not only enormous U.S. investments in sophisticated military systems but our future ability to project power into hostile airspace as well.

This book also documents many of the internal organizational and systemic failures that led to the embrace of a fundamentally irrational doctrine called "counterproliferation;" which is characterized by an escalating series of draconian responses to problems the United States has decided not to prevent. By gutting an effective export control regime rather than redirecting or reforming it we are left with

an option of last resort as our primary instrument of policy. By so doing, the administration has placed itself in the hypocritical position of supporting the wholesale transfer of U.S. equipment, technology, skills, and jobs abroad knowing that it, or an unfortunate successor, will one day come to Congress for its blessing to attack the military threat that will inevitably result from their policies.

This dramatic weakening of the international system of export controls lies at the heart of a series of independent developments that are gnawing away at our defense industrial base and are spilling over into our civil industrial base as well. Several parallel developments have long-term implications for the economic health and competitiveness of our economy as well as the safety of our men and women in the armed forces. They include:

- The open penetration of U.S. high-tech industries, and national and military labs by Chinese and other foreign nationals who carry home critical military or manufacturing technology

- The massive unilateral U.S. decontrol of supercomputers and supercomputer manufacturing technology (see Attachment A)

- The wholesale transfer of military factories to China, including a Columbus, Ohio, B-1 Bomber, C-17 Airlifter, and ICBM factory as documented most thoroughly in John Fialka's book *War by Other Means*

- The widespread auctions of defense manufacturing plant and equipment, often to foreign buyers, and the loss of skilled personnel, experience, and productive capacity for our industrial base (see Attachment B)

- Permitting Chinese agents to purchase state-of-the-art military parts, components, and weapons systems directly from DoD surplus property auctions, as reported by *U.S. News and 60 Minutes*

- Forcing the introduction of 'commercial-off-the-shelf' (COTS) technology into our weapons systems and the phasing out of MILSPEC requirements (see Attachment C)

- The flooding of the domestic and international market with state-of-the-art manufacturing equipment at cut-rate prices and the undermining of efforts to

strengthen the American machine tool industry

- The lease of the former Long Beach Naval Station to a shady arm of the Chinese government and the construction of a Chinese "Wholesale Mall" next door to the recently closed George Air Force Base in San Bernardino County, Ca. George AFB is strategically located 70 miles from the Navy's China Lake weapons development center, only 40 miles from the Palmdale stealth and "black program" aerospace test facility, and just 30 miles from Edwards AFB -- the primary U.S. military aerospace test flight center. George AFB has been selected as the production site for the "Predator" RPV, which will incorporate the most advanced sensor technology available. If a permanent PRC presence develops at such a strategic location it may offer China unparalleled eavesdropping and intelligence collection opportunities. (see Attachment D)

These are but a few of many datapoints in a massive process that is converting portions of the U.S. defense industrial base into the Chinese defense industrial base. Who knows what other PRC-related activities are developing at the dozens of recently closed military bases throughout the United States. With two more rounds of base closings proposed in the Quadrennial Defense Review the prospects are frightening.

Instead of preparing prescriptive remedies to serious potential threats, the administration diverts attention by focusing exclusively on small, almost irrelevant, pariah states such as Cuba, Syria, Sudan, Iraq, Iran, and Libya to deflect attention away from the fact that big money was being made modernizing our most likely future adversaries. Chief among them is China.

The consequences of the reckless dismantlement of the export control system may be seen even in the case of the pariahs. For example, much is made of Libya's installation of a chemical weapons factory inside a mountain but there is no discussion of how the Libyans were able to hollow out a mountain to create an impregnable fortress. Instead, official rhetoric is geared toward the further vilification of Qadhafi -- who needs no help qualifying as a world-class villain. A chemical factory is a standard part of the infrastructure of any nation with ambitions of economic development and import substitution. Unfortunately, most chemical plants are capable of producing chemical and nerve agents as well as pesticides and fertilizer. But this particular plant, located in a bomb-proof installation, is a different story. A simple air raid or stand-off cruise missile attack may not be capable of destroying this facility if the need arises. It is likely that only the introduction of

ground forces or the use of nuclear or other weapons of mass destruction can effectively eliminate such a target.

The key issue here from a technology security perspective is how they were able to hollow out the mountain and effectively constrain U.S. options? More than likely some form of Western-supplied tunnel-boring equipment was used to create this fortress. Although such equipment was removed from the export control system several years ago it is precisely this type of highly specialized tool that moves the factory from a tactical to a strategic response. Weigh for a moment the potential costs of requiring a company to apply for an export license against having to live with this latent threat.

Mr. Chairman, the greatest single point of failure in maintaining a credible export control system was the neutering of the Defense Department's traditional role as the conservative anchor of the process. This action was carried out very quickly by freezing DoD's key staff out of the chain of command and isolating them from the decision-making process within DoD. DoD abandoned its traditional role and instructed DoD employees to side with the Commerce Department and isolate the State Department and ACDA on many issues. This bizarre role change finds the State Department at times in the farcical position of being the lone agency making the national security case and opposing liberalization positions from DoD. An almost comical situation develops with the State representative scratching his head in bewilderment over how he wound up anchoring the right-wing view. I don't know about you, but I view reliance upon the State Department as the bulwark of our national security with more than a little disquiet.

Beyond these actions our strategic position is being further eroded from other angles. The much-ballyhooed "Dual-Use Initiative" was advertised as the Defense Secretary's plan to cut DoD procurement costs by using commercial technology in weapons systems wherever possible. This initiative is unfortunately a double-edged sword, which, while promising some potential cost savings, will also slash critical advantages in U.S. technological superiority by forcing weapons systems to use the same decontrolled technology potential enemies are now allowed to build their own weapons around. It also forces our military to rely upon critical microelectronics and components that are designed and manufactured abroad, thus making them extremely vulnerable to supply cut-offs, countermeasures, spoofing, or even sabotage. These are the very same dual-use technologies that the administration has actively decontrolled.

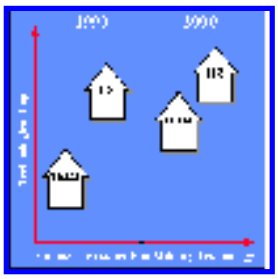
Threats to U.S. National Security

Former Secretary of Defense Dick Cheney observed in 1992 that "world events repeatedly defy even near-term predictions. In early 1989, few predicted Eastern Europe would escape Soviet domination by Thanksgiving. In early 1990, few predicted America would be headed for war by Labor Day, or would have half a million troops in Saudi Arabia by New Year's Day. Even at the end of that war, few appreciated the strength of Saddam's nuclear program. In early 1991, few predicted the Soviet Union would be gone by Christmas. In earlier times, we failed to predict the Soviet development of atomic weapons and Sputnik, the North Korean invasion of the South, or the Japanese attack on Pearl Harbor."[1], [2]

He also emphasized, "We field the most technologically advanced weapons in the world. This factor partially offsets the need to match potential adversaries' quantitative advantages. The combination of the technological superiority of U.S. military systems and the result of forty-nine years of preparation to fight a global war provided us with the capability to effectively contain and counter aggression."

However, current policies, which emphasize the funding of research and development activities but put production and implementation in abeyance, will further compound the erosion of the technology gap that the taxpayer worked so hard to achieve. Attachment D depicts the nature of DoD weapons development money and the firewall between R&D and mass production. One of the questions for your Committee to consider is whether the military need to fund the production of new systems would have been as soon, as expensive, or in as great a number had an effective non-proliferation regime been kept in place.

Unfortunately, the technological gap between the United States and many potential adversaries, in particular China, is closing from both ends of the strategic equation. Fold in the unabated takeovers of U.S. defense companies by foreign entities and the process accelerates further and takes on overtones of irreversibility.[3] My view of this relationship is depicted in a notional manner below and is expressed in a development economics context wherein many of the aforementioned factors contribute to the narrowing of the life or death technology gap historically enjoyed by the men and women in our armed forces.[4]



Click here to see Figure.

Technology and Weapons Systems

Technological superiority is not an absolute term. It is measured against an adversary's overall military capability. As such it is a fluid concept rooted in the state of technological development characteristic of *each* side, the degree to which the military capability of *each* side benefits from the pace of technological advancement, and the rate and extent of the metamorphosis of new ideas into *fielded* military systems.

In the United States, a major weapons system takes approximately fifteen years from initial concept formulation to introduction in the field. It is a well-accepted fact that military product development cycles in the United States drag on gruesomely long, usually resulting in military systems that incorporate electronic components several generations behind the existing state of the art. For example, it took eleven years for products incorporating the military's first very high speed integrated circuits (VHSIC's) to appear on the market even though the VHSIC program's major purpose was rapid insertion of advanced components in weaponry.[5] Even the top-billed U.S. defense weapons used in the Persian Gulf were not as modern or as sophisticated as much commercial technology. The much-acclaimed Patriot and Tomahawk missiles were developed over twenty years [earlier], and many of their parts are even older. For example, the 8088 microprocessor used in the Patriot missile was developed by the Intel Corporation fifteen years earlier.[6]

Unfortunately, the administration persists in clinging to a methodology that has no technical merit or basis; that is, the case-by-case judgment whether a particular technology transfer will close the technology gap between the recipient and the U.S. Unfortunately, the National Security Council and the Joint Chiefs of Staff applied this flawed concept in conjunction with the sweeping CoCom decontrols of 1990-92. This demonstrated a fundamental oversight, or lack of appreciation, of the incremental nature of technological advancement or the symbiotic relationship between disparate

technologies when incorporated into a weapons system. It is the amassing and integration of a variety of interdisciplinary building blocks that defines technological superiority. The persistent U.S. refusal to recognize these facts will guarantee the failure to protect critical military technology, which, in my view, will result in long-term strategic disadvantages and a future back-breaking burden for the taxpayer to desperately finance an eleventh-hour spending frenzy. (see Attachment E)

Underlying the administration's refusal to protect U.S. technology and our defense industrial base is the identity fallacy: the notion that big effects must have big causes, that big events must have big consequences, and conversely that small events must have small consequences. These assumptions are often erroneous and contrary to the principle of nonlinearity, which relates seemingly small events as essential catalysts to a degree of change well in excess of what may be expected by casual observers. Such a catalyst initiates a reaction among a series of independent, and seemingly unrelated, simultaneous events to create a nonlinear or disproportionate result. For instance, the assassination of the Austrian archduke in Sarajevo was only the catalyst that set in motion the chain of events resulting in the first World War. So, too, are the scores of relatively small, seemingly unrelated, military technologies released to potential adversaries over the past few years. Attachment F demonstrates the staggering consequences and costs that may result from the transfer of key enabling technologies. This notional study shows how the transfer of laser technology can be used against us and may force the redefinition of the nature of air combat, power projection, and even sensor technology.

The Central Intelligence Agency's Technology Transfer Assessment Center undertook the only known systematic attempt to array a variety of militarily critical technologies against the weapons systems in which they are found. The CIA data found in Attachment G underscore the pervasive nature of certain technologies.

These tables "relate all technologies to all military systems" and assign three levels of criticality to each entry: helpful, important, and essential. The CIA methodology draws strength from identifying "Western technologies and equipment which are required for the development and production of future Soviet military systems."[7] Unlike the current system, which is heavily biased toward developing a universal set of "militarily critical technologies," the CIA system returns to the original reason for U.S. and multinational export controls -- [foreign] military needs."[8]

Neutralizing Stealth

The cumulative effect of the unrestricted decontrol of technologies such as radars, computers, displays, traveling wave tubes, fiber optic cables,[9] signal/array processors, and software, and their incorporation into hostile military air defense networks, will be to neutralize the manned bomber component of the U.S. strategic triad and place in great jeopardy the multi-billion-dollar U.S. investment in stealth technology. The integration of these technologies make possible the detection and tracking of U.S. stealth aircraft. Conversely, the decontrol of composite materials, production equipment, and know-how will advance the stealth efforts of potential adversaries as well.

"Stealth" is neither a magical concept nor a black art. It represents the merger of a variety of new materials, long-standing engineering principles, and state-of-the-art computational modeling capabilities into an airframe capable of attenuating or deflecting radar impulses away from an enemy radar receiver.

If these transfers result in the loss of even one B-2 bomber, the financial loss alone would greatly exceed any potential profits to be realized by the sale of equipment. The loss of two B-2s would be the dollar equivalent of losing a nuclear-powered aircraft carrier with its eighty-plus aircraft aboard. In addition, the resulting erosion of the manned bomber leg of the U.S. strategic triad is of fundamental import to U.S. defense planning, yet the defense planning establishment, including Congress, was not a party to this decision-making process. Unfortunately, the ability to detect and track low-radar cross sections so critical to stealth detection is the same capability required for defense against cruise missiles.

Both of the stealth aircraft shown to the public so far (the Lockheed F-117A and the Northrop B-2) appear to be designed for intruder rather than air-defense purposes, but what is now obvious is that very low radar cross sections (RCS) are achievable. Reductions in RCS are the primary basis for achieving low observability, and the effect can be calculated quite simply because all radars conform to an immutable law of physics -- that detection range varies with the fourth root of the RCS measured in square units. For any given aspect, if the RCS is reduced by a factor of ten, then the detection range should be divided by 1.78. Thus, if an aircraft with an RCS of ten meters squared (m^2) could be detected at 100 nautical miles (nm) range, then a reduction to 1 m2 RCS will result in a pick-up range of 56 nm. A further reduction to 0.1 m^2 brings the range down to approximately 32 nm.[10] The two factors held to be of greatest significance in determining RCS are shape and the material used in the

object's construction. However, achieving true stealth is not just a matter of reducing the RCS. Other critical factors concern system design, including size, shape, aspect, and materials; and reduction of detectable noise (both acoustic and electronic), infrared emissions, and trails (smoke or vapor).

I believe that the two most devastating technology decontrols cover machine tools and high-speed computers (machine tools from two perspectives -- first, their ubiquitous presence in the manufacture of **all** advanced military systems, particularly where high precision or complex geometry is required. Second is their criticality to U.S. industrial competitiveness.

The U.S. strategic advantage over most foreign weapons systems relies on mission effectiveness and lethality, both of which develop at the subsystem level, contrary to the logic of the "gap-closer" approach, and saw ample demonstration in Iraq. For example, the so-called opto-mechanical devices found in advanced targeting systems are produced on machine tools in the ±5-9 micron range as are the miniaturized guidance systems in state-of-the-art missiles. In addition, critical components in advanced cruise missile warheads and "smart weapons" are produced on machines in the ±5-9 micron range.

The relationship ofÊcomputers and advanced machine tools to the proliferation problem is often posed in simplistic terms: *Since the U.S. did not need computers or computer-controlled machine tools to develop nuclear weapons and ballistic missiles, there is little need to control either technology for these purposes.* The argument ignores the fact that computers and computer-controlled machine tools have become an essential tool for many activities that were previously accomplished either by secretly amassing dozens of Nobel laureates, supported by hundreds of top physicists, in the mountains of New Mexico for several years or by metalworking artisans fashioning unique parts for small lot production. Computers and computer controlled machine tools have made themselves central by defining the very way technical goals are accomplished, and can substantially enhance the effectiveness of the limited pool of talent often available to a proliferant country while providing the capability for mass production of highly effective weapons systems.

Proliferant countries operate under constraints that the U.S. nuclear program did not: economic/political sanctions, lack of physical (test facilities, expendable fissile material, etc.) and/or financial resources, threat of possible pre-emptive attack by a concerned neighbor, etc., which would make computer simulation of paramount importance. This is also increasingly the case for ballistic missile testing as well, and

fewer tests will mean such programs are less visible, less vulnerable to international opinion, and more difficult to assess and guard against. Computers and computer controlled machine tools are particularly useful for the more advanced proliferants as they develop a more sophisticated military arsenal. At whatever stage of development, it is in the USG interest to make a weapon of mass destruction (WMD) and ballistic missile program as difficult, expensive, and unreliable as possible.

Decontrol by Metaphor

The unremitting drumbeat for decontrol is not without its creative side. Perhaps its greatest example was the clever use of simple terminology such as "hot sections" to mask radical decontrol measures which have swept away most restraints on the export of advanced propulsion technology. As displayed in Attachment H, using terms that have no intrinsic meaning has been an effective vehicle with which to decontrol the underlying materials, techniques, and equipment for the manufacture of even the most advanced military engine technology.

We've Heard This Song Before

While it is impossible to "child-proof" the world, strategic export controls have been, and can continue to be, an effective restraint on a potential adversary's ability to inflict grave military damage on the United States and its allies.

Mr. Chairman, the massive technology decontrols and the sell-off of U.S. defense assets throughout the mid-1990's [particularly to China] and the failure to recognize growing threats to our national security are chillingly reminiscent of the disastrous French armaments policies on the eve of World War Two. According to William Manchester in his excellent biography of Winston Churchill *The Last Lion*, in 1940, the French high command decided to sell its tanks abroad. The R-35 was a better tank than any German model. Of the last 500 produced before May l0, 1940, nearly half -- 235 -- were sold to Turkey, Yugoslavia, and Rumania, with the result that when the Germans struck only 90 were on the French front. Moreover, while Nazi troops, Stukas, and armored divisions were massing in the Rhineland for their great lunge westward, the generals charged with the defense of French soil gathered representatives of countries not regarded as unfriendly to France and auctioned off 500 artillery pieces, complete with ammunition, and 830 antitank guns -- at a time when the French army was desperately short of both weapons.

Perhaps even more to the point was the British cabinet decision in 1934 to sell 118 Rolls-Royce Merlin engines to Germany. You may recall that the Merlin engine became the principal powerplant in the Spitfire airplane that literally saved England from Hitler's advances and destroyed his plan to invade England just a few years later. In fact the Supermarine Spitfire is undoubtedly one of the most famous fighters of all time. When the Battle of Britain began on August 12, 1940, nineteen Spitfire Mk 11 squadrons and thirty -- two Hawker Hurricane squadrons stood to face the German onslaught. For the next 80 days, 3,500 German bombers and fighters fought against fewer than 1,000 Spitfires and Hurricanes as the most important battle of World War Two raged. The faster, more maneuverable Spitfires were used against fighters while the Hurricanes fought the German bombers. When the fighting ended on October 31st the Spitfires and Hurricanes had downed 1,733 German aircraft.

Manchester also documented how "Chamberlain had insisted upon approval of the sale as a matter of high principle and he stated 'trade, like religion, should recognize no frontiers.' The engines, he insisted, had been designed for civilian use, and he chose to ignore the fact that they could also be used in small fighter planes. When Churchill was informed of this export to Germany, he refused to believe it; until the actual bill of lading arrived in a plain envelope. Immediately he proposed a total ban on aircraft deliveries abroad. The Royal Air Force needed every plane it could get, he said, and none should be sold to any other country -- certainly not to Nazi Germany. Chamberlain, speaking for the cabinet, rejected his proposal because the trade policy of His Majesty's government required that 'deficiencies in the Defense Forces should be made up with the least possible interference with the export trade.'"

Chamberlain's obstinate refusal to face up to the reality of growing military threats to national security and the placement of the balance of trade and the short-term profits of private companies ahead of military preparedness is one of the hallmarks of current U.S. policy. The similarity in tone, manner, philosophy, and outcome between the two can be seen most clearly in the U.S. approach to China.

I am afraid that we are witnessing history repeat itself. Chamberlain called Churchill a warmonger for his warnings of the dangers posed by the German monster looming in the East. Chamberlain even came out and said, in 1934, that he could only base his decisions upon his predictions for the next two years. Looking beyond that limited horizon could not be done. Unfortunately, the United States is conducting its foreign and military policies in much the same myopic fashion. Preparing for future threats is given credence and funding only when it does not interfere with moneyed

interests or large adversaries.

Mr. Chairman, the fact that these hearings are being conducted today indicates to me that the foresight and courage that Churchill personified is present in these halls as well.

I would be pleased to answer any questions you may have.

Peter M. Leitner, *Decontrolling Strategic Technology, 1990-1992: Creating the Strategic Threats of the 21st Century*. Lanham, MD: University Press of America, 1995.

Endnotes

1. Peter M. Leitner, *Decontrolling Strategic Technology, 1990-1992: Creating the Strategic Threats of the 21st Century.* Lanham, MD: University Press of America, 1995.

2. Statement by Secretary of Defense Dick Cheney to House Budget Committee, (Feb. 5, 1992): 1-2.

3. Larry Skantze, "Prototype Mentality a False Path: U.S. Must Realize Technology's Value Lies in Exploitation," *Defense News* (September 10, 1990): 24; Linda Spencer, *Foreign Investment in the United States: Unencumbered Access*, (Washington, D.C.: Economic Strategy Institute, 1991).

4. The most critical feature is the expression:

$$MTC = [C, L, E, N, S] + \left(\frac{[I + DV + R\&D + P + IT + AT]}{Time} \right)$$

In the left side of this expression, MTC = Military Technology Capabilities. The first portion of the right side of the expression represents the traditional

building blocks of the economic development function, comprised of the following factors: C = Capital, L = Labor, E = Education, N = Natural Resources, and S = Sociological factors, i.e., birthrate, mortality, etc. The second portion accounts for those factors, beyond the building blocks, that are essential to the development of advanced military technologies. While not all-inclusive, they are representative of the major factors. These include the following: I = Industrial Base, DV = Diversification, R&D = Extent of resources dedicated to military research and development, P = Political will to sustain activity, IT = Indigenous technology, AT = Access to relevant foreign technology. The factors are bounded by Time.

5. Michael Borrus and John Zysman, "Industrial Competitiveness" *Rethinking America's Security: Beyond Cold War to the New World Order*. Graham Allison and Gregory F. Treverton, eds., New York: W.W. Norton and Company, 1992, 173.

6. Ibid., 123.

7. U.S. Central Intelligence Agency, *National Security and Export Controls: A Decision Aid*, (Undated, Circa. 1990): 1.

8. Ibid., 1.

9. Michael S. Lelyveld, "Fiber-Optic Curbs on Ex-USSR Tied to Missile Fear," *Journal of Commerce*, (March 24, 1992), 1.

10. M. B. Elsam, *Air Defense*, London: Brassey's, 1989, 78.

Return Home

Statement by

Mr. John J. Fialka

before the

Joint Economic Committee
United States Congress

June 17, 1997

CHINA AND ECONOMIC ESPIONAGE

Spies are normally associated with wartime and the theft of military technology. In the vast popular literature about espionage, there is hardly a mention of peacetime economic spies. One reason may be because spy stories tend to blossom when wars end. War is relatively clear cut: there is a winner and an eventual loser; a beginning and an end. The end is normally the signal for the memoir writers to begin.

But economic espionage is different. Winners win quietly and losers are often either unconscious of loss, or too embarrassed to admit it. My book argues that this is like a war because war-like damage can result, but there is no beginning, no end, and, consequently, no memoir writers. As far as I know, my book is the first thoroughly-documented book on the subject.

Although few Americans are aware of it, our nation's history has been heavily influenced by economic espionage. Shortly after the American Revolution, we were the spies. And the richest, most industrialized part of the world at that time--Europe--was our target. Alexander Hamilton, Thomas Jefferson and many others among the founders' generation were involved in it, but one American spy stands out--Francis Cabot Lowell. He managed to steal the design of one of Great Britain's technological marvels, a water-powered loom that was so efficient that it could produce acres of cloth with relatively little human labor. Using this technology, Lowell created the New England textile industry which was, in turn, the foundation for America's

industrial revolution.

One hundred and eighty four years later, the world that Mr. Lowell knew has been stood on its head. What he managed to start, the American industrial economy, is now the richest in the world. As such it has become the chief target of the world's economic spies. There are quite a number of them--from at least 20 major countries. Meanwhile, Americans have become complacent. Unlike our ancestors, who scoured the world for new ideas, we have lost our hunger for that. Many of us have come to assume that the best technology will always be here.

The thesis of my book is that that assumption may no longer be true. Unless we can understand the efforts currently being made against us and raise our awareness to the point where we win at least as many episodes as we lose, we will be in serious trouble. The National Economic Council, which includes experts from the CIA, FBI and the Departments of Treasury, State, Defense, Commerce, Justice and elements of the White House prepared a secret estimate of the current situation for Congress's intelligence committees in 1994. The report says that "economic espionage is becoming increasingly central to the operations of many of the world's intelligence services and is absorbing larger portions of their staffing and budget."[1]

This could involve a lot of people and a lot of power because nations have brought a their Cold War spy apparatus with them into economic espionage including giant computer data bases, word-activated eavesdropping scanners, spy satellites and an almost unbelievable array of bugs and wiretaps.

Economic espionage carried out in the U.S. breaks down into three major styles. The study says agents from China, Taiwan and South Korea are aggressively targeting "present and former nationals working for U.S. companies and research institutions." Japan, which does not have a formal intelligence agency but sometimes collectively resembles one, uses Japanese industry and private organizations to gather "economic intelligence, occasionally including classified proprietary documents and data." The result is an exceptionally efficient spy network that "is not fully understood" by the U.S. Meanwhile, France has relied upon "classic Cold War recruitment and technical operations," which generally include bribery, discreet thefts, combing through other peoples' garbage and aggressive wiretapping. There are recent signs, however, that France has decided to stop.

Another Cold War ally, Germany, is described as planning to increase the number

of its Federal Intelligence Service (BND) agents in Washington to improve its collection capabilities. And Russia and Israel also conduct economic intelligence gathering operations in the U.S. with "varying degrees of government sponsorship.[2]

The most aggressive operations against U.S. companies occur overseas, especially in home countries where spy agencies are freer to act and where, the National Economic Council report notes, "government controlled national phone networks" and other electronic means can be used to slither inside company communications and data banks. The best places to recruit foreign nationals who work for U.S. companies overseas is said to be in third countries where "a host country's counterintelligence services do not pose a serious barrier to effective foreign intelligence operations directed against U.S. targets. Furthermore, U.S. citizens tend to be more lax about security matters when living in countries perceived as friendly to the United States."[3]

"Lax" is probably a polite way to describe the laid back attitudes that many Americans have toward our technology. A recent study by the National Research Council found that one way Japanese businessman collect information about the U.S. aerospace industry--one of Japan's current major targets--is to get their U.S. counterparts to brag. "Ego comes into play as engineers try to impress their foreign contacts..."[4]

Part of Japan's approach is simple: they have many more people looking here than we do there. In 1988 Japan sent 52,224 researchers to the U.S. Meanwhile 4,468 U.S. researchers went to Japan.[5] Japanese companies invest the time and money to teach their people English and the U.S. culture. U.S. companies rarely bother.

And what Japan has accomplished in the U.S. has caused a stir of envy, especially in the Peoples Republic of China whose collection efforts in the U.S. are likely to be larger and, in the long run, more threatening than the Japanese campaign, which they appear to be using as a model. Like Russia and Japan, China's initial target has been U.S. universities. In 1991, 51 percent of all science and engineering doctorates awarded by U.S. universities went to students from Pacific Rim nations with the dragon's share going to the two Chinas. Many of these students--educated largely at the expense of the U.S. government--get jobs in the U.S. after obtaining their doctorates and a large number of high tech companies and U.S. government research laboratories are becoming hooked on this stream of cheaper, often smarter and more biddable talent.[6] Some of these students eventually become U.S. citizens and help

renew the American dream by achieving breakthroughs that mean new jobs and new markets. But many go back and government recruiters from their homelands are working here to lure more back home, where they become serious and sometimes dangerous competitors. What makes this scary is that while the influx of foreign students has been growing, the faltering U.S. public education system has been producing fewer and fewer qualified applicants for graduate level science and engineering. What this means is that many new U.S.-invented technologies that we expect to drive our economy in the 21st century--such as biotechnology and photovoltaics--are being quietly targeted and exported overseas.

My book shows how the Japanese, Russians and the French do economic espionage, but I would like to keep this testimony focused on China, which poses problems that, I think, will become more serious over time. In this game China is a dragon with two heads. Other competitors look for commercial advantage, China, a nuclear power, looks for that as well as military advantage and they often find both in the same deal. Its commercial companies are often parts of its military. They have tank companies that sell us teddy bears and toilet seats. Their profits from the U.S. go to modernize a Army, Navy and an Air Force that has begun to flex its growing military muscle in the Pacific. China's prime intelligence agency, the Guojia Anquan Bu, or Ministry of State Security (MSS), has flooded the U.S. with spies, sending in far more agents than the Russians even at the height of the KGB's phenomenal Cold War campaign. About half of nine hundred illegal technology transfer cases being investigated on the West Coast involve the Chinese. The MSS recruits students. When money is not persuasive, threats against family members back home often are. And unlike the KGB, China's spies easily find protective cover in the large U.S. Asian population.[7]

While the FBI makes an effort to watch foreign students and businessmen, China's flood has simply overwhelmed the bureau. "The FBI is ensnarled in a cess pool of Chinese agents and their cases are all stuck at first base," says James Lilly, former U.S. ambassador to China and former CIA station chief in Beijing.

While the Japanese focus on things like disc brakes and video cassette recorders, China's strategists shop for missile guidance systems that can use signals from our satellite-based global positioning system for precise targeting information. They go after small cruise missile engines, night vision equipment, upper stage rockets and nose cones for globe-spanning nuclear weapons. These are all things that may fundamentally shift the balance of power in the next decade and drive threatened countries like Japan and Taiwan into full-blown nuclear weapons programs.

You will find that a lot of trade experts and business executives don't see and don't want to see this side of China's balance sheet. The prevailing intellectual fashion is to regard the lowering of trade barriers and the influx of foreign goods and students as part of a vast, multi-cultural economic march toward a peaceful "globalism." Increasingly, sovereign issues such as national borders, intelligence and military matters are dismissed as old hat.

But they are not old hat to China's current leadership, which is using a whole range of Cold War espionage tactics, such as the insertion of "sleepers," or long term spies, against the U.S. Federal Court documents in Norfolk, Va., show how one young Chinese philosophy professor, Bin Wu, was sent to the U.S. under orders to become a successful businessman, to steal weapons-related technology and to develop political sources in the U.S. Senate and the White House. Before he was sent, he was told that the U.S. was one of the major enemies of China, and that China was preparing for a "long battle." As his U.S. career blossomed, he was told by his MSS handlers, he would never be alone. "Someone will always be worrying about you."[8]

China's Ministry of State Security was formed by combining the espionage, intelligence and security functions of the former Ministry of Public Security with the investigations branch of the Communist Party's Central Committee. What had been largely an internal instrument used to hunt down and annihilate political dissidents in China, was recalibrated to work abroad. In its modern form it supports its budget by hunting here for technology like its model, the Soviet Union's huge, far-flung KGB.

Bin Wu's case was a classic spy recruitment, a process that is known in the intelligence trade as putting an agent "under discipline." Wu, who had been under investigation in China for political crimes, was hooked through a combination of personal fear, threats against his family and the other baits they had dangled before him. While many other nations recruit spies in this process, China's operations are different because the MSS recruits armies while other nations field platoons. A former FBI official told me: "A lot of people are using their intelligence agents to collect from us in the economic area, but the Chinese do it like a fare thee well. The Chinese are a giant vacuum cleaner."

Because China currently floods the U.S. with 15,000 students a year and recruits its agents from among the candidates being considered for student visas, a Defense Intelligence Agency expert estimates there could be "a minimum of several hundred

long-term agents operating here."[9]

U.S. intelligence agencies have discovered that one of the MSS's many skills is getting the U.S. to pay most of the costs of their espionage. China and other Far East countries are believed to siphon money from consulting firms they form to help U.S. companies create business ties abroad. The money is then used to finance espionage in the U.S. "We tell U.S. businesses this activity is going on," says Robert A. Messemer, a former FBI counter intelligence expert in Los Angeles. "Many of these efforts are directed at the very same companies that they are cooperating with overseas...they're funding the operations that are being run against them."

Another favorite Chinese tactic is squeezing defense-related high technology out of U.S. companies as a necessary part of business deals. One incident that is currently being investigated by a federal Grand Jury in Washington began on August 1993 when a group of Chinese visitors entered a U.S. defense plant, called Plant 85 in Columbus, Ohio. One of the visitors carried a video camera and slowly panned down the length of some of the factory's biggest machines. They were from a subsidiary of China's National Aero-Technology Import & Export Corp. (CATIC), which deals in both military and civilian equipment.

This was a very bold move. The machinery CATIC's team was eyeing amounted to an entire military aircraft plant, the largest east of the Mississippi. It would be impossible to steal it and smuggle it out. It would be illegal and impolitic for China, on its own, to try to buy it and ship it out. Some of the equipment could machine metal to tolerances so precise that they were on the U.S. State Department's list of "very sensitive" technology. Whoever had them had the capability of machining state-of-the-art nuclear warheads.

But CATIC had found another way. It was trolling an enormous bait, a $1 billion aircraft order in front of McDonnell Douglas. The hook was that, to get the order, the U.S. aircraft company would have to make the political case in Washington to get the export licenses that were was necessary to ship the machines to China.

The pull being exerted by China on U.S. companies is enormous. For many of them, China is the moon and they hope to ride on the tides created by a growing market of 1.2 billion people. Because China doesn't recognize a lot of U.S. business law, dealings there can pose enormous risks. It is a place where business, military and criminal deals often intermingle. By some measures China is one of the most corrupt

places on the planet.[10] Nonetheless, business there still remains tempting. "The only thing worse than being in China is not being in China," Edgar S. Woolard Jr., the chief executive officer of Dupont, once reasoned. "If your competitor catches on there, they're going to come after you with this enormous base."[11]

Much of what U.S. aerospace companies have to sell has "spun off" of U.S. military technology. In China, U.S. military experts have begun to notice something they call "spin-on." As the Chinese learned how to make fuselages and nose cones for McDonnell airliners, for example, emerging versions of Chinese fighter planes had fuselages that were better made and aluminum skins that were smoother.[12]

The team from CATIC offered to buy Plant 85's best machines for roughly 10 cents on the dollar. While it looked like the start of a commercial deal, CATIC is simply not another widget company. It is part of China's aviation ministry. It can apply the leverage of a government agency, which is what it is. It has the technological knowhow of a big defense contractor, which develops fighters and missiles for China's Air Force. It is developing a keen sense of the world's commercial markets: CATIC runs some 66 commercial companies, whose profit-making business ran from making airliners to running luxury hotels and shopping centers to making fashionable watches.[13]

CATIC's sister agency, the Peoples Liberation Army, runs over 10,000 private businesses. They export a wide spectrum of commercial products, from tea sets to fork lifts, many of which are sold in the U.S. Part of the money is then used to modernize China's sprawling military--the largest in the world. Just how much money flows from the commercial businesses of China's government into the business of developing new weapons is a mystery, but it is probably a substantial sum. U.S. analysts believe that as much as two-thirds of China's defense budget is hidden.[14]

McDonnell officials told Craig M. Ziegler, an investigating U.S. Customs agent, that the plant's most sophisticated machines, called "5-axis profilers" were not being offered to CATIC.[15] Then CATIC raised the ante. It said a failure to sell the machines in Plant 85 would have a "big influence" on the $1 billion plane deal and future deals with China.[16]

After that, McDonnell's position appears to have been hastily revised. "We always wanted to sell them (China) the machines," explained Tom Williams, a spokesman for McDonnell. As for the peculiar back-and-forth in the negotiations and

the threat imperiling the $1 billion plane deal, Williams dismissed it as "normal." "If you have ever bargained with the Chinese, they are always picking up and leaving the room."[17]

Thirteen of the plant's sensitive five-axis machines were sold after CATIC promised to use them only to make parts for the McDonnell-designed airlines, The Clinton Administration approved the sale on the rationale that the U.S. needed the sale to help offset what was then a $30 billion trade deficit with Beijing.[18] (The deficit is now approaching $45 billion.) Although many items in this avalanche of imports were produced in Chinese military factories, Clinton Administration economists ignored that.

The matter of why China needed these machines is a question that should not be ignored because it probably has military, not commercial significance. For reverse engineering, you only need one machine to make copies. China's buyers were collecting dozens of them as Cold War-era controls relaxed. By the winter of 1993, U.S. intelligence agencies estimated that China was in the process of importing some 40 of the big machines, counting the ones in the McDonnell deal. It was an amount that seemed far beyond the commercial needs of China's fledgling aircraft industry, or any other industrial country in the world, according to one U.S. official. What is going on?

One theory is that China is gearing up to export a large number of airliners, sales that would compete directly with Boeing and McDonnell. Another is that China is preparing what U.S. defense planners call "surge capability," the capacity to produce a large number of high technology military planes and precision-guided missiles in a hurry. What is worrisome to experts in the Pentagon is that, when it comes to China, the two goals are not incompatible. There is plenty of evidence that Beijing wants both guns and butter.

Pentagon experts, trying to block the sale, argued that as far as high technology military equipment is concerned, China is a sieve that steadily leaks it into the Third World. It has sold missile guidance systems and computerized milling machines to Iran and missiles and a jet trainer powered by a U.S.-designed engine to Pakistan. F. Michael Maloof, the Pentagon's director of Technology Security Operations asserted that once Plant 85 machines arrived in China, the U.S. had no way to keep them from being put to military use.[19]

McDonnell replied that it "has been assured by CATIC that this factory will only produce parts for civil aircraft."[20] When it took an inventory of the machines, however, it found two of them in Nanchang at an aircraft facility not covered by the agreement. The Nanchang factory makes cruise and ballistic missiles. "That was not a proper end use, so that was rectified," explained Williams, the company's spokesman. According to one government official, McDonnell's way of rectifying matters was to ask the U.S. Commerce Department to suspend the export license it had granted for the machines--a move of dubious value since the machines were already in China, somewhere.

In the summer of 1995, Barbara Shailor, an official of the International Association of Machinists and Aerospace Workers, watched two U.S.-built five-axis machines--which, she was told, also came from the batch shipped from Plant 85--being installed at a plant in Xian, in China's heartland. The plant's workers, who make approximately $50 a month, were working simultaneously on the B-6D, a medium range, nuclear weapons-carrying bomber, making tail sections for the Boeing 737, and planning for a new airliner, which could be largely indigenous. She asked a technician for an American company working at the plant whether the two-headed nature of the plant bothered him. "Everything around here is dual use," he shrugged.

The final mechanism that China uses to find and siphon away U.S. technology is its enormous stock of students studying here. Again, it is borrowing from Japan's model. While Japanese students were flooding the campuses in 1981, the Peoples Republic of China had no doctoral candidates in the U.S. Ten years later it had 1,596.[21]

The Chinese students tend to be super-bright, an elite skimmed from a nation of over 1.2 billion people.[22] There are so many of them that they have come to dominate the lower levels of faculties in many universities and they regularly win highly-prized research and teaching assistant ships, which means that they teach and have the keys to the laboratory and that their education is subsidized by the schools and U.S. taxpayers. It has reached the point where American undergraduates frequently complain that they can't understand their teacher's English.

The idea that the U.S. can manage its growing dependency on these students is still popular on U.S.campuses. One reason is that it fits the needs of many senior U.S. scientists, who can select brighter researchers from overseas to do their research

papers and their teaching, often at a fraction of the cost of a U.S. student.

For years the myth has been that most foreign science graduates remained in the U.S. The U.S. Immigration and Naturalization Service kept no records on it. "It's not something we're interested in because it doesn't help with our work," explained a spokesman for the agency.[23] But recently Michael Finn, an economist at the Department of Energy's laboratory at Oak Ridge, Tenn., found a way to test the myth. Checking students' Social Security numbers ten years after graduation, he found that between 50 and 60% percent of the graduates no longer worked in the U.S.

"We definitely hear more anecdotal evidence that foreign countries are putting more efforts into recruiting students to come back," says Finn. One exception is the Peoples Republic of China which, according to Finn, appears to have made a decision to keep a pool of talented scientists working in U.S. companies and university laboratories, a pool that China can draw on later.

One reason may be that the U.S. pays their salaries as they continue to learn. Plus, according to Finn, the "vast majority" of Chinese students in U.S. science and engineering schools are supported by assistant ships or other means provided by the universities, usually through U.S. government funding.[24]

Mr. Finn's agency worries that the dwindling number of U.S. scientists and engineers may mean that the nation will no longer have enough native-born scientists to work on classified weapons projects. When you think about it, that is a problem that should give us all pause.

You have decided to hold these hearings at an historic moment. For the first time in almost decade there appears to be growing awareness among the American public that China may not be the most exemplary trading partner. It continues to trample the human rights of its own people. It continues to proliferate weapons of mass destruction in the Middle East. It sends spies to steal U.S. weapons technology--which amounts to an act of war. At the same time, it makes secret moves to deny U.S. companies access to its markets, such as telecommunications. And now, in addition, we see a growing body of evidence that it has tried to manipulate the U.S. political process to its own advantage.

The question facing you is whether we continue to appear numb to this threat, or whether we do something that tells China it must modify its behavior. "Trade

experts" would have you believe this is an enormously sensitive, touch-me-not question. In its simplest form, I'm not so sure that it is. Remember the third grade? What happened to you if you continued to appear weak and stupid in front of the class bully? Was that complex? No, it was predictable. You lost your lunch money.

In past history, we protected our companies by erecting a wall of tariffs. I think that age is past, but selected trade barriers, such as removing China's most favored nation status, would send the message that our laws and our commercial and political processes must be respected, not abused. In the long run, however, I think the best defense will be an offense. We must make ourselves better, more world-savvy competitors. Companies should understand when they lose, we all do. Like some companies do now--notably Kodak and Motorola--they must be willing to take the fight overseas, studying foreign cultures to find legal means to learn what their competition is doing. Here, companies must also become more willing to bring cases to court, using new laws such as last year's Economic Espionage Act to create a body of case law and an actuarial basis for risk can be used by insurance companies to help protect people. Lessons are not learned if you hide them.

Companies and the government must also be made aware that reliance on foreign scientists to develop and guard our secrets is--as the Romans once discovered--a short-run fix. In the long run we will either fail as a leader of technology, or we will have to restore our broken public school system so our students can continue to compete with the best in the world. As a body, China's students here are exemplarily people that we can learn much from, but among them are some spies, people whose assigned mission is our downfall. As Francis Cabot Lowell once vividly demonstrated, we should never lose sight of that. Nations that take their technological edge for granted have a great deal to lose.

Endnote

1. Report on U.S. Critical Technology Companies, Report to Congress on Foreign Acquisition of and Espionage Activities against U.S. Critical Technology Companies, 1994, p.5

2. Report on U.S. Critical Technology Companies, p.23.

3. Ibid, p. 25.

4. "High-Stakes Aviation: U.S.-Japan Technology Linkages in Transport Aircraft," p. 88.

5. U.S.-Japan Technology Linkages in Biotechnology, National Research Council, 1992, pp. 34-35.

6. North, David S., Soothing the Establishment; The Impact of Foreign-born Scientists and Engineers on America. p. 78 & ff.

7. Eftimiades, Nicholas, "Chinese Intelligence Operations," Naval Institute Press, 1994, p.17 and p. 27.

8. The account of Wu's meeting at the Old Cadre's club comes from the trial transcript of U.S. vs. Bin Wu, Jing Ping Li and Pinzhe Zhang, CR 92-188-N, U.S. District Court for the Eastern District of Virginia, Norfolk, Va. The trial was held in May, 1993.

9. Eftimiades, op. cit., p. 67.

10. Transparency International, a Berlin-based group dedicated to curbing corruption in international business transactions, ranks 41 countries on a "corruption index," based on polls, reports of businessmen and business journalists. With a possible high score of 10, China scored 2.16, ranking it just above Indonesia, which was in last place.

11. Woolard made his remark in November 1995 at a symposium on international security issues at the State Department.

12. "Civil-Military Integration; The Chinese and Japanese Arms Industries," a background paper published by the Office of Technology Assessment, a branch of the U.S. Congress, in 1995, p.142.

13. "CATIC; United, Realistic, Competitive, Innovative," brochure produced by CATIC, undated.

14. "Impact of China's Military Modernization in the Pacific Region," U.S. General Accounting Office, June 1995, p. 18.

15. Report by Ziegler to the director of the Strategic Investigations Division, U.S. Customs Service, Oct. 4, 1993.

16. Letters exchanged during the negotiation were later released by the Pentagon.

17. Interview with Williams, October, 1995.

18. "China Swiftly Becomes An Exporting Colossus, Straining Western Ties," Wall Street Journal, Nov. 13, 1995, p. A1.

19. China's position, according to Li Daoyu, its ambassador in Washington, is that it has "all along adopted a serious and earnest attitude toward the issue of non-proliferation and opposed the proliferation of all weapons of mass destruction pending their complete elimination globally." Arms Control Today, op. cit., p. 9.

20. "Background--CATIC Machining Co. Ltd.," part of McDonnell's application for an export license for the Plant 85 machinery submitted to the U.S. Commerce Department.

21. "Foreign Participation in U.S. Academic Science and Engineering: 1991," special report by the National Science Foundation, February 1992, pp. 28 and 85.

22. Some come from China's military elite. Gen. James A. Williams, former head of the Defense Intelligence Agency, recalls a chat with a number of lieutenant colonels in the Peoples Liberation Army during a visit to Beijing in 1983. They spoke with American-accented English and talked about their days on U.S. college campuses. When he returned to the U.S., Gen. Williams, now retired, had their names checked against U.S. immigration records. There were no records. "All I can figure is that they must have come in under different names," says Williams.

23. Interview with INS spokesman, April 4, 1994.

24. Interview with Finn, Sept. 1995.

Return Home