

**ECONOMIC ESPIONAGE, TECHNOLOGY
TRANSFERS AND NATIONAL SECURITY**

HEARING

before the

**JOINT ECONOMIC COMMITTEE
CONGRESS OF THE UNITED STATES**

ONE HUNDRED FIFTH CONGRESS

FIRST SESSION

JUNE 17, 1997

Printed for the use of the Joint Economic Committee



U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1997

cc45-119

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-055880-8

2
J841-4

JOINT ECONOMIC COMMITTEE

[Created pursuant to Sec. 5(a) of Public Law 304, 79th Congress]

HOUSE OF REPRESENTATIVES

JIM SAXTON, New Jersey, *Chairman*
THOMAS W. EWING, Illinois
MARK SANFORD, South Carolina
MAC THORNBERRY, Texas
JOHN DOOLITTLE, California
JIM MCCREERY, Louisiana
FORTNEY PETE STARK, California
LEE H. HAMILTON, Indiana
MAURICE D. HINCHEY, New York
CAROLYN B. MALONEY, New York

SENATE

CONNIE MACK, Florida, *Vice Chairman*
WILLIAM V. ROTH, JR., Delaware
ROBERT F. BENNETT, Utah
ROD GRAMS, Minnesota
SAM BROWNBACK, Kansas
JEFF SESSIONS, Alabama
JEFF BINGAMAN, New Mexico
PAUL S. SARBANES, Maryland
EDWARD M. KENNEDY, Massachusetts
CHARLES S. ROBB, Virginia

CHRISTOPHER FRENZE, *Executive Director*
ROBERT KELEHER, *Chief Macroeconomist*
HOWARD ROSEN, *Minority Staff Director*

Prepared by Juanita Y. Morgan

CONTENTS

OPENING STATEMENTS OF MEMBERS

Representative Jim Saxton, Chairman	1
Senator Jeff Bingaman, Ranking Minority Member	4
Senator Charles S. Robb	4
Senator Jeff Sessions	33
Representative John T. Doolittle	37
Senator Robert F. Bennett	40

WITNESSES

Statement of Dr. Peter M. Leitner, Author of <i>Decontrolling Strategic Technology 1990-1992: Creating the Strategic Threats of the 21st Century</i>	4
Statement of Lieutenant General Robert L. Schweitzer, United States Army (Retired)	10
Statement of John Fialka, Author of <i>War by Other Means: Economic Espionage in America</i>	15
Statement of Kenneth Flamm, Economist, Brookings Institution ..	20

SUBMISSIONS FOR THE RECORD

Prepared Statement of Representative Jim Saxton, Chairman	59
Prepared Statement of Dr. Peter M. Leitner, Author of <i>Decontrolling Strategic Technology 1990-1992: Creating the Strategic Threats of the 21st Century</i>	62
Prepared Statement of Lieutenant General Robert L. Schweitzer, United States Army (Retired)	119
Prepared Statement of John Fialka, Author of <i>War by Other Means: Economic Espionage in America</i>	128
Article "Controlling the Uncontrollable," submitted by Kenneth Flamm, Economist, Brookings Institution	138

ECONOMIC ESPIONAGE, TECHNOLOGY TRANSFERS AND NATIONAL SECURITY

Tuesday, June 17, 1997

**CONGRESS OF THE UNITED STATES,
JOINT ECONOMIC COMMITTEE,
WASHINGTON, D. C.**

The Committee met pursuant to notice, at 10:05 a.m., in Room 138, of the Dirksen Senate Office Building, the Honorable Jim Saxton, Chairman of the Committee, presiding.

Present: Representatives Saxton and Doolittle, and Senators Bingaman, Robb, Sessions and Bennett.

Staff Present: Christopher Frenze, Mary Hewitt, Roni Singleton, Juanita Morgan, Howard Rosen, and John Blair.

OPENING STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

Representative Saxton. Good morning. Thank you very much, everyone, 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 those policies' impact on our economy, particularly in the context of the legislative intent of the authors. The areas of concern that I have learned of have 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 age of changing reality of a former Soviet Union, an emerging Asia and a struggling, sometimes unstable Third World.

I am pleased to welcome to the Committee an extremely knowledgeable group of panelists. Let me introduce them.

Dr. Peter Leitner is the author of a new book entitled, *Decontrolling Technology: Creating the Military Treaty for the 21st Century*. I would

like to make clear that Dr. Leitner will testify as the author of that book and not in his official capacity as Foreign Trade Advisor to the Department of Defense.

Additionally, Dr. Leitner is the author of the book, *Reforming the 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 Lieutenant General Robert Schweitzer, retired. 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 Medals, two Legion of Merits, the Distinguished Flying Cross, the Soldiers Medal, the Bronze Star with Valor device; three additional awards, the Air Medal with Valor device, seven Purple Hearts and two Army Commendation Medals. That's quite a list, Lieutenant General Schweitzer. And, we are pleased to have you here.

General Schweitzer will testify 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 the Russians to a variety of countries. The weapon is the Radio Frequency Weapon, known as RF, on Electromagnetic Pulse weapon used, among other things, to cripple computer capability.

It has only been in the last few weeks that some 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*. He is the author of *War by Other Means*, an important but disturbing book on high

technology 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 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.

He 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 a book, *Hotel Warriors*, which is an analysis of the press coverage of the Persian Gulf War.

Our final panelist is Mr. Kenneth Flamm. Mr. Flamm has been working as Senior Fellow at the Foreign Policy Studies program at the Brookings Institute since 1995, a position he 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 for Dual Use Technology Policy. At Brookings, Mr. Flamm has also focused much of his research on international competition in high technology industries.

Let me add a 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 illegal activities would not be countered.

I look forward to the enlightening testimony from our panelists.

And, at this time, I will turn to the Ranking Member for any comments he may have.

[The prepared statement of Representative Saxton appears in the Submissions for the Record.]

**OPENING STATEMENT OF SENATOR JEFF BINGAMAN,
RANKING MINORITY MEMBER**

Senator Bingaman. Mr. Chairman, I don't have any comments. I am looking forward to hearing from the witnesses. And, I appreciate them all being here.

Representative Saxton. Are there any other opening comments?
Senator Robb.

OPENING STATEMENT OF SENATOR CHARLES S. ROBB

Senator Robb. Thank you, Mr. Chairman. I look forward to the hearing.

As one who serves on all three of the National Security committees as well as the Joint Economic Committee, this is a particularly important topic for me. I will not be able to remain for most of the testimony.

I will take it with me, and I will rely on the record. But, I thank you for calling the hearing.

Representative Saxton. Senator, thank you very much. Dr. Leitner, why don't you begin?

And, we are anxious to hear from you and any comments that you may have which may shed light on the subject that we are here to examine today.

**OPENING STATEMENT OF DR. PETER M. LEITNER,
AUTHOR OF *DECONTROLLING STRATEGIC
TECHNOLOGY 1990-1992: CREATING THE
STRATEGIC THREATS OF THE 21ST CENTURY.***

Mr. Leitner. I appreciate it. 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.*

I need to state up front that the opinions, as you have said already, and analysis I express here today are my own and do not represent the views of the Defense Department, the U.S. 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 originally in writing this book stemmed from the dramatic politicization of the export control process. I have seen the blatant manipulation of honest technical, engineering and intelligence 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. This campaign 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 cutouts 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.

The current Administration was responsible for the elimination of CoCom before any replacement regime was installed. The result was the loss of any potential negotiating leverage in ensuring that a follow-on regime would have any teeth.

The unnecessary destruction of CoCom opened the floodgates of technology to China, among others, as it was subject to few restraints other than in the narrow realms of ballistic missile and nuclear technology. As the Chinese already are 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 the quest for a few hundred million dollars in potential sales, we have made available the means to offset not only

the enormous U.S. investments in sophisticated military systems but our future ability to project power into hostile territory as well.

The book also documents many of the internal organizational and systemic failures that led to the embrace of a fundamentally irrational doctrine called "counter-proliferation," 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.

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; 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; 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 World Report" and "60 Minutes;" forcing the introduction of commercial-off-the-shelf technology into our weapons systems and the phasing out of MILSPEC requirements; the flooding of the domestic and international market with state-of-the-art manufacturing equipment at cut-rate prices from these plants that are being shut down and the undermining of efforts to strengthen the American machine tool industry (and we have become a direct competitor with new machine tool production); and, finally, the lease of the former Long Beach Naval Station to a shady arm of the Chinese government, which we are all aware of, and now the proposed

construction of a Chinese wholesale mall next to the recently closed George Air Force Base in San Bernardino County, California.

As you can see by this chart, George Air Force Base is located right in the heart of the U.S. advanced aerospace development activities. This whole development complex, including stealth research, stealth design activities and radar cross section test ranges. It's near Edwards Air Force Base where most of the advanced aerospace platforms are tested and worked out and also not far from the telemetry which is pervading the atmosphere from the Pacific Missile Test Range and other things.

George is also the home of the future production of the Predator, the remote piloted vehicle, which our military force is going to rely upon for intelligence and communications capabilities in the future. The Chinese characterization of this area as "treasured land" is understandable.

If a permanent PRC presence develops there, it may offer China unparalleled eavesdropping and intelligence collection opportunities. These are but a few of the many data points 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 is being made modernizing our most likely future adversaries. Chief among them is China.

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 key DOD staff out of the chain of command and isolating them from the decision-making process within DOD.

DOD abandoned its traditional role and instructed it's employees to side with the Commerce Department and isolate the State Department and the Arms Control and Disarmament Agency 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 where the State Department representative is sitting 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.

Underlying the Administration's refusal to protect U.S. technology and our defense industrial base is the identity fallacy – the notion that small events must have small consequences. These assumptions are often erroneous and contrary to the principle of non-linearity, which basically says that small events can act as catalysts to very large change.

The charts show the staggering consequences and costs that may result in the transfer of key enabling technologies. This notional study, which I have submitted for the record, 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.

Next is an example of a \$40 million airplane flying against a \$50,000 laser weapon to drop \$20,000 worth of high explosives on a target. There is something very wrong with this arithmetic.

The effect of laser blinding is quite dramatic on pilots. And, unfortunately for the pilot, his eyes are a sensor just as his FLIR and his other equipment on board are sensors. And, they are very vulnerable to laser radiation.

The technology to do this has been decontrolled and is available worldwide. The cumulative effect of the unrestricted decontrol is one of the things I want to talk about, also, the costs associated with this.

The cost of countering the potential \$50,000 laser blinder may run into the tens of billions of dollars, particularly if you engage in frequency shifting. Or, if you have developed an agile laser that can operate across the various parts of the electromagnetic spectrum, it is almost impossible to defend against. Some of the costs and possible solutions I have evidenced in this chart to explain that in greater detail in the record.

The cumulative effect of the unrestricted decontrol of technologies such as radars, computers, displays, traveling wave tubes, fiber optic cables, signal and array processors and software and their incorporation into hostile military air defense networks may be to neutralize the

manned bomber component of the U.S. strategic triad and place in great jeopardy the multibillion-dollar U.S. investment in stealth technology as well. The integration of these technologies makes 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.

If these transfers result in the loss of even one B-2 bomber, the financial costs alone will greatly exceed any potential profits to be realized from the sale of equipment. The loss of two B-2s would be the dollar equivalent of losing a nuclear-powered aircraft carrier with its 80-plus aircraft aboard.

I believe that the two most devastating technology decontrols cover machine tools and high-speed computers.

The unremitting drumbeat for decontrol is not, however, without its creative side. Perhaps the 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.

The gas turbine engine technology, et cetera, is basically at risk, at very serious risk, for missiles, cruise missiles, aerospace, et cetera.

I want to wrap up with a historic analogy of what happened in France prior to World War II when the French were auctioning off their artillery, their tanks and their antitank weapons, just on the eve of the German invasion. As a result, what was already a shortage became an absolute scarcity on the French front when the Germans did attack. The U.S. is operating in a similar fashion today.

One of the best examples was a confrontation between Churchill and Chamberlain, where Chamberlain was trying to sell Rolls-Royce Merlin engines to the Germans. Churchill got wind of it and tried to stop the sale, saying, "These are absolutely critical. We don't want to arm the German monster that's looming in the east." There ensued a great debate and a great fight where Chamberlain basically was arguing the same issues that are argued today, that trade, like religion, should know no boundaries and deficiencies in the armed forces should not be made up at the expense of the export trade.

Chamberlain even said that his predictions could see only two years into the future in determining what the threats would be and what policies should be. That's remarkably similar to the time frame that the Clinton Administration has chosen to decontrol computers and technology. Two years in advance of their actually even being invented, trying to predict what the market is and decontrol them two years in advance.

The last comment I would like to make is on what occurred yesterday. There would be quite a few DOD employees in this room in attendance today were they not explicitly banned from attending by DOD officials who issued orders yesterday that they are not allowed to attend this hearing, even though it directly affects their jobs and what they do, and if anybody applied for annual leave to attend this hearing it would be denied. It's rather bizarre. And, it was referred to the DOD Inspector General for investigation yesterday afternoon.

Mr. Chairman, the fact that these hearings are being conducted today indicates to me that the foresight and courage that Churchill personified in the 1930s and '40s is present in these halls as well. And, when the time comes, I will be pleased to answer any questions anybody has.

Thank you.

[The prepared statement and charts of Mr. Leitner appear in the Submissions for the Record.]

Representative Saxton. Dr. Leitner, thank you very much. General Schweitzer, we are pleased that you are here today. And, we are anxious to hear your statement at this time.

OPENING STATEMENT OF

**LIEUTENANT GENERAL ROBERT L. SCHWEITZER,
UNITED STATES ARMY (RETIRED)**

Mr. Schweitzer. Thank you, Mr. Chairman. I am going to try to put, just in a few minutes, the work of a year and to summarize, in a little bit short fashion, what will be the white paper that will be offered to the Department of Defense on this whole subject.

What I want to concentrate on, because of the nature and character of your Committee and the work of it, is the impact of these new weapons of which I will be speaking on the infrastructure, because that is totally missing from consideration right now. I'm going to talk today

about a radical new class of weapons, radio frequency weapons, which, as you said, Mr. Chairman, have been wrapped in mystery and secrecy for many years. This should not be the case.

The Internet has literally tens of thousands of documents on radio frequency weapons. Articles and books are written on it. There are many unclassified statements in the public record by Department of Defense officials.

I find, in that regard, some 90 to 100 references to this threat – and that's really what it is – in the Quadrennial Review, although nowhere is the term, "radio frequency weapons," used. But, asymmetric threats, discontinuous threats, the new technologies, the way we will have to deal with them.

For the military, if I can illustrate the whole thing by putting you all on the deck of the Forrestal in July of 1967, F-4s were loaded in the Gulf of Tonkin with armament ready to go out on their missions. Radar sweeping the deck, scanning it, found some faulty shielding in one of the F-4s.

And, in a second, a missile was loose, rolling across the deck and within just moments we had an absolute conflagration and which took about seven months for the Forrestal to be repaired. And, 134 officers and sailors lost their lives all because of a demonstration of quantum physics and electrical engineering which can and have been applied to create weapons.

And, this history goes back before anything – any accident of electronic interference on the Forrestal. It goes back to Japan and World War II where they created the first radio frequency weapon that was used and didn't even know they had done it. Their work began in 1927.

There are many scholars and scientists who have worked on this. In fact, one of our problems with technology transfer on this, as I say in my written statement, the horse is out of the barn. The transfers have been going on in this area at least since 1949 when the first international conference in Frascati, Italy took place where these ideas were shared. And, the work then synthesized and came forward.

Anyone can attend these conferences. The Russians were at the first one. They are vigorous participants in all of them.

There is a BEAMS conference that has gone on for 20 years, a EUROEM conference that has gone on for over 20 years under different names.

In its 1994 meeting in Bordeaux, France, the Russians laid out the fruits of their work up until then, which included a very detailed description of a whole series of radio frequency weapons and papers that gave the strategy, doctrine, tactics and techniques as to how they would be used. Now, I am not a "the Russians are coming" speaker today. This is not the threat.

They are our friends, and they are working with us at least now. And, we hope that will continue.

In fact, one way to do it, in my belief, is to engage in joint ventures with them on these very weapons, because they are engaged in proliferating them. At the Bordeaux conference, Iran and Iraq attending, picking up the papers, they were - the Russians were in the business of negotiating transfers and sales of the technology and the weapons.

Our own work here in the United States is really noteworthy. I have been down to the laboratories in Senator Bingaman's state. I am very impressed with the brilliance of the quality and the dedication of the scientists at both Sandia and Los Alamos.

At Los Alamos, this month, they are taking a Russian design, fabricating the weapon themselves, but it's a Russian weapon that they are fabricating. They are convinced that it will perform to the standards and capabilities of the - that the Russians are claiming.

There is a lot of dispute about what the Russians claim. After a year of work on this, I am convinced, along with the famous Dr. Max Fowler, who invented the first RF weapon in the United States at Los Alamos, that what the Russians say they do, they have proven; what they have promised, they have tested out at Los Alamos.

There are other tests that will be taking place, one out at another national lab in the west where young engineers accepting a challenge that we, at least, made in part to them, went out to Radio Shack and bought components to make a RF weapon, mounted it on top of a minivan. I had suggested a pickup truck and they didn't have a pickup truck, so it went on top of a minivan.

And, this device will be tested also this month. I am convinced that this will work.

And, the cost is about \$800 to do this. These weapons, therefore, at low power have an enormous impact on the infrastructure.

And, I would like just to cite some of the things that they could do to the infrastructure. They can affect the national power grid, anything that has got an electronic chip in it, a circuit board, any piece of electronic gear that is touched by one of these weapons. And, they come either as narrow beam over long distances or ultra-high beam, ultra-wide beam, ultra-wide ban weapons that can project greater rates of power.

You don't need a lot of power to affect the infrastructure. The military has a problem - my army, as we modernize, miniaturize and micronize all of our equipment, it becomes more vulnerable to RF weapons.

So, this whole new trend in information warfare that's so good and which we are embarked on so successfully has a backside to it. Unless you protect the systems, they are more vulnerable.

And, in the economic infrastructure, with which this Committee is so much concerned, there is no hardening at all. There is no protection against RF weapons.

So, you've got a situation on the one hand where you could put components from Radio Shack inside of a van no bigger than a UPS truck with the antenna. And, that's really what an RF weapon often looks like, a radar or an antenna showing, and drive it around the Dirksen Building, make a series of passes over the Pentagon or the White House or the FAA facility out at Langley and pulse.

And, the wonderful thing about these weapons, from a scientific point of view, is they have deep magazines. They don't require any ammunition. They can fire, refill as long as there is power in that generator.

You make a number of passes around the building and emit these pulses. They go through concrete walls. Barriers are no resistance to them. And, they will either burn out or upset all the computers or the electronic gear inside the building.

The way they are designed in the work that is being done in the United States, they are absolutely safe. And, everything I am telling you, incidentally, is unclassified.

They are absolutely safe to human beings, because they meet the standards of protection for humans. So, that's an advantage. They have become a nonlethal weapon in that sense.

But, the danger to the military of these weapons appearing on the battlefield is probably somewhere off in the future, I think nearer than most people do but off in the future. But, for the infrastructure, it's here now.

Anybody - in fact, one quote from one of the engineers was, "Any idiot can go and build one of these weapons."

You can use them against the banking system so that currency transactions and financial transactions cannot be made. They can be used with these intense pulses to attack railroad and transportation systems.

Everything depends on electronics to pass trains and shuttle them back and forth and even more so for airplanes, which is always kind of a sensational subject in the inventory target for terrorists. These weapons can interfere with the takeoff and landings of airplanes. They can bring an airplane down.

Indeed, there is one incident, the only one the National Transportation Safety Board has not ever concluded on, other than the one in New York where they have reached a provisional finding, but this was out in Colorado Springs in 1993. And, it had the earmarks of an RF weapon, other than nobody ever came forward to take the credit or the blame for having done it.

You can disrupt the pressure and flow in the petroleum pipes and in the gas and oil lines. You can interfere with traffic lights and cause gridlock.

You can cause nuclear power plants to malfunction, to go into shutdown. You can cause files and data, any digital data, to be corrupted or changed or altered.

The telecommunications we share, military and civilian. Ninety percent of our military traffic goes over civilian lines, so it's hard even to define infrastructure.

There are some recommendations. We need a policy lead - and I will conclude with this. I hope to get your questions to go into more detail.

We need a policy lead in the Pentagon and in the government to provide direction, which is now wanting, not that it can't be given and certainly not that it shouldn't be given. But, we need a strong policy lead.

And, that's one of the reasons why these matters haven't come to light sooner and been addressed better.

I would also like to conclude by saying the one thing that worries me is that as we go into an R&D phase, which the Russians are doing, increasing their budget – one study says six-fold, another two-fold in this area. And, the one, for me, disturbing thing in the Quadrennial Review was the statement that we were going to consider a base realignment and closing to include the national labs.

We are going to need those labs to come up with the inexpensive solutions – and many of them are – for protection with plasma limiters, surge protectors, metal covers. There are a number of things. Even paint will work in some cases.

We need, I believe, to get the labs involved in this in finding the solutions. And, the one thing that should not be displeasing to you is this is not a budget buster.

It's going to take time just to get our arms around the problem, at least a year. It's going to take time to test to get the vulnerabilities and susceptibilities and then look at the different systems to protect what we have.

Thank you, sir.

[The prepared statement of Mr. Schweitzer appears in the Submissions for the Record.]

Representative Saxton. Thank you very much, General Schweitzer.

Mr. Fialka, we are interested, obviously, to hear your statement this morning. So, why don't you proceed at this time?

**OPENING STATEMENT OF JOHN FIALKA, AUTHOR OF
*WAR BY OTHER MEANS: ECONOMIC ESPIONAGE
IN AMERICA***

Mr. Fialka. Thank you, Mr. Chairman. As you know, I am a reporter with the *Wall Street Journal*, so I want to emphasize that today my remarks are as the author of *War By Other Means: Economic*

Espionage in America, which is the first documented book on economic espionage.

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, Great Britain, was our target.

Alexander Hamilton, Thomas Jefferson and many others among the founders' generation were involved in spying. But, one American spy stands out. His name is 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 reasonably little human labor. Using this technology, Lowell created the New England textile industry which was, in turn, the foundation for our industrial revolution.

One hundred 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, we are the chief target of the world's economic spies. They come from at least 20 major countries.

Meanwhile, Americans have become oddly 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 National Economic Council, a branch of the White House, has prepared a secret estimate of the current situation for Congress' intelligence committees in 1994. The report says, "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."

It says economic espionage carried out in the United States breaks down into three major styles. 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 large formal intelligence agency but sometimes collectively resembles one, uses Japanese industry and private organizations to gather economic intelligence.

Meanwhile, France has relied on "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 revised its thinking on this and has decided to stop, at least for the moment.

Russia and Israel have conducted economic intelligence gathering here for many years with varying degrees of government sponsorship.

My book shows how the Japanese, the 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 than all the rest.

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 here in the same deal.

One method that they use involves the insertion of sleepers or long term spies against the U.S. We have one case that has been exposed in federal court in Norfolk, Virginia, showing how one young, Chinese philosophy professor, Bin Wu, was sent to the United States 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. Those were his specific orders.

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 handlers from the Chinese Ministry of State Security he would never be alone, "Someone will always be worrying about you."

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 dangled before him.

A Defense Intelligence Agency expert, whose name is Nicholas Eftimiades, estimates there could be a minimum of several hundred long term agents, sleepers, operating here on behalf of China.

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 here by a federal grand jury began on August 1993 when a group of Chinese visitors entered a U.S. defense plant, called Plant 85, in Columbus, Ohio. It was operated then by McDonnell Douglas.

The Chinese were from a subsidiary of China's National Aero-Technology Import and Export Corporation known as CATIC, which deals in both military and civilian equipment. It was a very bold move.

The machinery CATIC's team was looking at amounted to an entire military aircraft plant, the largest east of the Mississippi. It would have been impossible to steal the machines in that plant.

Some of them could machine parts to tolerances so precise that they were on the State Department's list of very sensitive technology. Whoever had them had the capability of machining state-of-the-art nuclear warheads.

But, CATIC found another way. It told McDonnell Douglas that \$1 billion aircraft order from them stood in the balance. They could either have the order or not, but if they wanted the order they had to provide the machines and make the political case in Washington to get the export licenses.

McDonnell Douglas, which at first told its union it was not going to sell the machines, reversed its position and sold them. They arrived in China.

And, then they began appearing at military facilities where they were not supposed to be. And, that's the part of it that is still under investigation.

The third arm of Chinese effort – of China's effort – here involves Chinese students in the U.S. It has an enormous stock of students here, some 15,000.

They tend to be among the brightest people in the world, an elite skimmed from a nation of over 1.2 billion people. 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 assistantships, 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 students from overseas to do their research papers and their teaching, often at a fraction of the cost of a U.S. student.

The myth has been for years that most of these students remain here and become part of the American dream. The fact is that new research shows that at least half of them go back to build competitive commercial companies in Asia and some of them to build competitive weapons systems.

I must underline that most of these students are honest, hard working people. But, they provide cover that the KGB could only have dreamed of for a few spies that undoubtedly are among them.

You have decided to hold these hearings at a historic moment. For the first time in almost a decade, there appears to be a 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. And, now, in the John Huang case, 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. But, 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 complicated? 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 has passed. 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 and not abused or exploited.

In the long run, I think the best defense will be an offense. We must make ourselves better and more world-savvy competitors.

Thank you very much. And, I look forward to your questions.

[The prepared statement of Mr. Fialka appears in the Submissions for the Record.]

Representative Saxton. Thank you very much, Mr. Fialka. Dr. Flamm.

**OPENING STATEMENT OF KENNETH FLAMM,
ECONOMIST, BROOKINGS INSTITUTION**

Mr. Flamm. Thank you very much, sir. My name is Kenneth Flamm.

I'm an economist at the Brookings Institution. My particular area of expertise is high technology industry.

I've written a couple of books on the history of development of computer technology globally and on the economic history of the computer industry. My most recent work at Brookings has been on a book called "Mismanaged Trade," a definitive study of U.S./Japanese competition in semiconductors.

I served in the Department of Defense from 1993 through 1995. And, I was directly involved in and, to some extent, responsible for some of the decisions that led to the system of computer export controls that is being discussed today.

And, I am going to focus my remarks on computer export controls rather than the complete diversity of topics you have heard today, because it's something I know well and I think is, in some cases, being discussed in the absence of accurate information. So, I would like to just lay out the facts of what's going on in the computer industry today and how it relates to our system of computer export controls.

I would like to start out by talking a bit about where the industry is today. When I came into the Pentagon in 1993, the supercomputer export control line was 195, what are called, MTOPS, millions of theoretical operations per second, which is a somewhat arcane measure of computer performance that is used for export control purposes.

I would like to point out today that you can go to Best Buy over in the Pentagon City mall and buy a computer with an MTOPS rating

exceeding the supercomputer line in 1993 for about \$2,000. That's how quickly the technology has changed.

That's how important it was when we came in to do something to make those lines more realistic. Well, I will return to this subject later.

Let me talk for a moment about what a supercomputer is if we are going to talk about controlling exports of supercomputers. A supercomputer has always been a relative term.

It refers to the highest performance computing machines of the day. It has changed over time.

The fundamental thing that has driven the constant revision of the definition of what is a supercomputer is the fact that technology has moved so quickly in this industry. Every 18 months or so, the performance of high-end computers has roughly doubled. That's just to give you some idea of how quickly this is moving.

When I came into office in 1993--now, in addition to my testimony, sir, I have also introduced a little chart, which I think I will be referring to and I think you will find useful, called "A Brief History of MTOPS," which points out where the supercomputer and other computer performance levels were, when using this MTOPS measure for different types of computers at various points in time when the supercomputer policy was being discussed. And, it also points out what the control lines were for that technology at the time this was being discussed.

When I came in 1993, a single Pentium personal computer, which was being introduced, actually was on the market, had an MTOPS rating of 66. A so-called work station, a high end work station, used for scientific work had an MTOPS rating of about 1,800. And, high end U.S. commercial supercomputers had an MTOPS rating of about 20,000.

Today, just by way of contrast, those numbers look like something like 350 for a single Pentium personal computer; about 1,500 for an easily constructed multiple processor work station made by a Korean company; about 32,000, 30,000 or so, for a high end server or work station on the market; 284,000 MTOPS for a high end U.S. commercial supercomputer that you can just go out and order and buy.

The machine that we are currently using at Sandia for nuclear weapons simulations of the sort that we are talking about, for nuclear stockpiles stewardship has an MTOPS rating that exceeds 643,000 MTOPS. So, these are the relative numbers.

In any event, when I came into DOD in 1993, it was clear that we had a problem. The decontrol level was 12.5 MTOPS.

As you can see, a single Pentium personal computer that was going to be shipped on the market in tens of millions of units had a power level, an MTOPS rating that exceeded five times what that decontrol line was. And, it was clear that within the next couple of years there were going to be four processor Pentium machines introduced on the market, which clearly were going to be exceeding the supercomputer line. And, these are not high technology. These are things that could be assembled essentially by a knowledgeable electrical engineer with a screwdriver, a soldering iron and a basic knowledge of the components that are available freely on the open market.

So, that was our problem. Basically, we were looking at a situation in which foreign computer companies, companies in Taiwan, companies in Korea, were essentially going to be given a protected safe harbor to compete against U.S. companies in what were clearly emerging, rapidly growing markets.

The computer industry has always been vital to U.S. national security. Mr. Leitner asked earlier how is it that the Department of Defense came to conclude that lowering the bar for controls on computers might actually be in the interest of the U.S. national security. The answer, quite frankly, is that the U.S. national security is tied to a computer industry that has global dominance.

We want to have access to the best, most powerful supercomputer technology in the world. The economics of the industry are such that export markets are a critically important part of U.S. industry sales, in excess of 50 or 60 percent of U.S. industry sales.

And, the only way we are going to be able to maintain that global dominance, from a national security perspective, is if our guys, our producers, continue to blow away the competition around the world. And, that means access to those export markets.

And, that means not setting up protected little enclaves where foreign challengers can prosper and grow and challenge our companies. So, that's the logic.

To put it another way, using Mr. Fialka's language, if we are the English steel mill - no, not steel mill, water driven textile mill, excuse me, and the basic principles for textile mills are becoming known, how do you protect your technical lead in textiles? Do you build a large wall

around your textile mill or do you rapidly improve that technology and continue to drive that technology forward as quickly as possible so that your textile mills are the most efficient, productive, highest tech, highest quality product lines in the world that continue to blow the competition away.

And, DOD, of course, concluded that to stay ahead in the technology was the smart way of staying ahead in the high tech game.

Now, when we approached this problem in 1993, looking at the reality you see in your table here, there were essentially three principles that we adopted in revising these export control levels. The first principle was: Don't waste effort or resources on trying to control what is essentially uncontrollable.

That technology was out there in the market. If the Taiwanese and the Koreans and the Poles, for example, can produce the product, there is really not a lot of point in putting resources into trying to control that level of technology.

The second point we made was that because this is such a rapidly moving industry, if you put a policy into place that is geared to what is out there today at this instant and it's going to take you two years to revisit those controls, (because that's the minimum gestation period that we've seen in the government) trying to impose a new set of control lines on computer technology, well, then, this technology is moving so fast you are essentially creating those protected niches for foreign competitors and giving them a toehold that is going to allow them to challenge U.S. computer companies and the hegemony, if you will, of U.S. computer technology, and that is not in the national security interest.

So, our second principle was that it ought to be prospective; that is, we ought to look out over the reasonable time frame it's going to take us to get around to looking at those technological controls again and look at something that is forward-looking, that recognizes the changes in the technology.

And, quite frankly, it's not rocket science to figure out where the technology is going to be in two years. Typically, in the computer industry, the products that you see rolling off with regular frequency month after month after month are in the pipeline for a considerable period of time before they roll off into the commercial market.

The new processor technology, the new computers that are coming out, they are in development for awhile. It's no big trick knowing what's

going to be rolling out on to general sale 18 months from now, because those products are being worked on and developed right now in the companies.

So, looking out 18 months to two years is not rocket science, particularly when you work closely with the manufacturers and your guys are the leaders in the industry.

The third principle we adopted in 1993 was to focus on what was of real military significance. That is, the whole point of this is not just control in computers because they are high tech, the whole point of the control system is to control those particular sets of technologies which are linked to significant military advantage.

So, the basic principle ought to be: Look at the military significance of what you are controlling. Try to pick those items that are focused, targeted and can have some real impact on the relative constellation of forces from a national security perspective - a sensible principle, I submit to you.

And, I think this, fundamentally, is what we ought to be talking about.

Now, let me just turn to the most recent round of decontrols we did, which was in 1995. We retooled the lines that were being drawn.

We had a new problem in 1995. A new so-called paradigm was occurring in the computer industry. That is, we were shifting from computers which essentially had a single or a small number of processors to massively parallel computers with large numbers of processors.

And, furthermore, off-the-shelf components that could be used to link computers together to provide large aggregates of computing power, or networks, from computers being linked together were developing very rapidly. And, it became clear to us that essentially there was going to be a massive multiplication of processing power.

And, essentially, we went out and we looked at these issues. And, we came up with two conclusions.

First of all, our studies showed that it seemed to be clear that by 1997 the U.S. industry and others were going to be shipping work stations in the range of 15,000 MTOPS. In retrospect, that proved to be a conservative assumption.

In fact, what is shipping now is about double that, 30,000 MTOPS.

And, we also, essentially, ended up concluding that 7,000 MTOPS would be available worldwide. The bottom line is we drew some new lines which made some sense.

I don't have time right now to go into the logic. It's described in my testimony, which I have submitted for the record.

The final point I would like to make today is that there is an awful lot of rhetoric about supercomputers that I think is irresponsible, in the sense that it's making factual statements that just aren't right. For example, it has become common now to hear in the local media that we sold 46 supercomputers to China since our last period of decontrol, and that this is more computing power than is in use in all the supercomputers within DOD. The absurdity of these statements is readily evident by just looking at the numbers.

This uses the old definition, for the 46, of a supercomputer, which is 2,000 MTOPS. The machines that recently have been the subject of controversy are 5,000 or 6,000 MTOPS. If you just look at where the MTOPS ratings are for supercomputers that are used by DOD today, the patent foolishness of this kind of claim is readily evident.

In conclusion, I would simply like to ask the Committee to focus on two things. Firstly, the fact that U.S. dominance in this area is an asset enormously important to national security as well as being of obvious economic benefit to the U.S. economy; and, secondly, there ought to be three issues we focus on in discussing export controls: One, what is available from the other guys out there in the marketplace that's going to be available whether or not we sell it to them; two, does this make sense? Are we looking forward to what we can reasonably predict is going to be going on in the next year or so in the marketplace? And, thirdly, what is of real military significance?

Those are the three issues. And, those ought to be guiding our discussion of what the control lines are and where we ought to be going with our export control policy.

Thank you.

[The prepared statement of Dr. Flamm appears in the Submissions for the Record.]

Representative Saxton. Thank you very much, Dr. Flamm. We appreciate all of your obviously very articulate and informed testimony on these very important subjects.

Let me just pose a question to Dr. Leitner and Mr. Fialka, because I want to make this point very clear. It is true, is it not, that the issue of technology transfer is not something that has come about in the last several years or even in the last decade?

As General Schweitzer pointed out in his testimony, pre-World War II Germany and pre-World War II Britain, saw technology transfers from different perspectives. And, it was an issue then to the Prime Minister.

And, so it is true that technology transfer, whether we talk about them for economic purposes or for military purposes, is an issue that has been around for a long, long time; is that – that's a fair statement?

Mr. Leitner. Yes.

Representative Saxton. And, so during the last decade or so, when we begin to focus on technology transfer, particularly military technology transfer, we have focused in the Bush Administration and now in this Administration on some aspects of military technology transfer that had to do with China, that is not a unique situation necessarily to this Administration. It was also a situation that occurred, to some extent, during the Bush Administration.

Is that fair to say?

Mr. Leitner. Yes, sir.

Representative Saxton. I just want to make that point, because we are not here this morning to look at this Administration or the last Administration or even this decade or the decade before it. This is a historic issue today which has ramifications, perhaps, that it didn't have in the past, but it is an issue that transcends time. It is important, however, that we look at in today's context.

Now, Dr. Leitner and Mr. Fialka, your testimony was similar in some respects, in that you both focused on the transfer of today's American technology to other countries through various techniques that are used by various people in the world who would like to have our technology.

And, Dr. Leitner, you focused on the transfer of that technology through some fairly obvious means, particularly with regard to China who would like to have and has obviously been fairly successful in gaining some of our technology. You mentioned COSCO. You mentioned bases which are in the process of being closed and propose some threat, therefore, to others taking over certain aspects of them.

And, Mr. Fialka, you mentioned the spy system and sleepers, about students. And, so there are certain aspects of the transfer of technology which would seem fairly obvious to someone like me. If COSCO is, in fact, locating themselves in certain areas to be – if they are, in fact, locating themselves in strategic position so that they can take part in this escapade, that seems fairly obvious.

On the other hand, students don't seem as obvious. So, we've got a broad spectrum of issues that we ought to be aware of and be looking at.

So, my question is: Given the wide range of issues that are involved here, what course or courses of action do you see that we ought to take in order to remedy the situation or begin to remedy the situation?

Dr. Leitner, why don't you go first? And, then, Mr. Fialka, why don't you go second?

Mr. Leitner. Thank you, sir. The first thing to do in order to come up with a prescriptive remedy for a problem is to understand its full dimension. And, in order to do that, one has to really sit down and organize a study of some sort that's going to be conducted in a non-political manner without the salesmanship evident, by some statements, trying to promote one particular industry over other industries in the United States.

And, the bottom line has to be what is U.S. technological superiority now and what is going to be needed in the future. And, once that benchmark is established, what likely threats are we going to face, what threats are posed by the particular countries like China, that is of concern right now, and what will be the critical technologies required to close a technological gap between us and them? These are critical points that have to be fleshed out. So far, it's totally absent from any of the planning.

I would really recommend that a Team B sort of approach, which was done quite successfully at the beginning of the Reagan Administration, be carried out again, except this time I would have it anchored in the Legislative Branch where oversight and additional players can be brought in to contribute to the process. The Team B approach would be to look at this problem with a fresh new cut and try to determine, through the impaneling of experts, through bringing in people from the Executive Branch on a selective basis, people from the intelligence community, people from the private sector and defense

contractors as well, as to where the future threats are. And, then try to put your arms around the problem and embrace it.

I've heard rumors in the past of other methods being used by the Chinese. One I found particularly disturbing was asserted once by a customs agent that there have been incidents - I haven't seen any recorded documentation of these incidents - where very young looking Chinese students were going to the United States and placed in high schools in the United States, except that their age was really 25 or 24 years old. And, there were false statements made on documents. Then they went into high schools and excelled. These were brilliant students. "Look at the brilliant student we have here from the People's Republic of China. He's acing his SATs. He has done remarkably well. He is getting into Stanford and MIT. And, isn't this remarkable?"

Well, it turns out that it's an example of a sleeper agent, somebody who is put in a position. He already has advanced degrees before coming in, then is put into the position as a seed and then is allowed to flourish in a totally unfair competition with U.S. student counterparts.

These techniques of the type that Mr. Fialka has pointed out, and others, really have to be understood and they have to be uncovered. And, the Team B approach I really think is the best way to go about it.

Just take a fresh look at the reality of the problem and its contextual realities without all the hyperbole, without the salesmanship, without the sponsorship where they are trying to promote a particular product as the be-all and end-all, and also take into account the technological gap that's closing quite rapidly, which U.S. military forces are going to suffer from in the future. This country is going to suffer. It is not going to be able to introduce force where it needs to introduce force, because we are not going to have the technology to overcome in an austere location far from home a modernizing military threat at that part of the world.

I would look into such issues as the new Chinese presence on both sides of the Panama Canal at Cristobal and Balboa. I would look at the growing Chinese presence in the Spratley Islands and now the new Chinese base construction in the Coco Island, a Burmese island on the other side of the Strait of Malacca.

Those two events alone should cause a great deal of concern, that two of the most strategic critical waterways that are the home of most U.S. maritime traffic and that of our allies, particularly for oil shipments and commercial shipments, are now being bracketed by Chinese presence

on either side. Now, is this just coincidental or is it going to lead to some sort of conflict?

Do they have plans for disrupting commerce and transportation in the Indian Ocean and the commerce between us and the Japanese? What is going on?

Is anybody looking at this? I have seen absolutely no sign that anybody is doing a comprehensive, strategic analysis of these various events.

Representative Saxton. Thank you very much. Mr. Fialka.

Mr. Fialka. Mr. Chairman, I think what has changed in your lifetime and mine is that in every previous war we went into, we went into with a strong technology base based on our own science. And, today, in the last ten years, that has radically changed.

If you look at the number of degrees awarded in American institutions, advanced degrees in science and engineering, 51 percent now go to students from the Pacific Rim with the majority of them coming from China. This means that they have an access in our laboratories that no potential competitor, either commercial or military, has ever had before.

The reliance is such that if you go to Sandia or Oak Ridge, you will meet senior U.S. scientists who are concerned that like many U.S. aerospace and defense corporations they may have to hire foreign scientists, visiting foreign scientists, to work on classified projects because the number of American students interested in science and engineering has dropped off a cliff. This is a first for us.

Some people would argue we are exporting our scientific base. Other people would argue that's silly, economic nationalist nonsense; this is pure global markets operating.

But, I would argue that if we can't compete in this area, if we can't fix our broken public school system and get more American students interested in science and engineering, we will lose this lead that we have often assumed has been there in our lifetimes. And, that's a major challenge.

It would require a lot of fixing. But, it's worth the effort. And, I don't think you have to be an economic nationalist to maintain that. I think it just makes good common sense.

Representative Saxton. Thank you. General Schweitzer, I take it that RF (radio frequency) devices are not new technology and the use of radio frequency is not something that we have just recently discovered. As a matter of fact, we have used radio frequency to jam signals between adversaries for many, many decades.

But, what makes it unique, I suppose, today is that the type of radio frequency weaponry that we can use applied to modern technology (i.e., computer chips) creates a much more intense and difficult situation for us to contemplate. To help us understand this, it occurred to me, as you were testifying, that there are a variety of ways that a country can be befuddled.

One of those ways would be, as you mentioned briefly - and this is something that I think many Americans would be interested in, you talked about interrupting banking operations. What would happen if a radio frequency device was used in downtown New York on Wall Street?

Does today's technology, RF technology, have the capability of having a dramatic effect such as shutting down Wall Street?

Mr. Schweitzer. Yes, sir. And, it's not these exotic weapons that I was talking about coming out of Russia.

That can be done with going to Radio Shack and buying the components. I have in my briefcase a catalog from one of the companies that is putting out these devices that says, "We will show you how to do it. Everything is included. If it isn't, we will help you get it with diagrams or other assistance." And, the prices are from \$35 to \$200 to buy components to go and do a number on Wall Street.

The kind of scenario that one could envision would be the van with a radio frequency weapon in it and no exterior signs or indicators or signatures on it, just driving in circles or up and down the canyons of Wall Street pulsing with this almost limitless capacity to generate high power pulses through the walls of the financial and banking institutions on, let's say, a Sunday morning at 2:30 a.m. And, you can make as many passes as you need.

So, if you have a weapon, as we do in our military inventory, with a certain probability of hit - let us say it was only 10 percent and, of course, ours are much higher than that, but if you had 10 percent probability of target effect and you made ten passes, you would greatly increase your target effect, which is not to say that the intelligence that you would need as to where every computer is located in every bank and

every financial institution would be available to the one or two people in the van doing this, the driver and one man inside generating the pulses. But, if you make enough passes and you propagate enough high-powered pulses through those walls, you are going to do considerable damage. You will either burn out or upset all the electronics.

Now, if a computer goes down in one of your offices and you have the technician and the spare part, you can fix it in five minutes. But, if you put down a whole system like that, a whole series of things – and the more damage you do, the more complicated things are to repair – then you've done considerable damage over a period of time.

And, this is not just speculative on my part. A year ago this month in London – and it's disputed in the Intel community and elsewhere but I think frankly, after having gone into this in great detail, the dispute is to protect the fact that it happened. But, the *London Times*, which is no tabloid, reported in June in 1996 that attacks had been made on their banking and financial institutions, enough to demonstrate the capability to do the damage. And, then they extorted by blackmail an enormous sum of money, 40 million pounds Sterling.

I was told that was a hoax. A week later, there was a story saying, no, the London government was seriously investigating this and, yes, these things had happened.

And, yes, this is a good way for people who have these weapons to gain money and funds through extortion. You don't even have to do it. You can shut it down either deliberately to do the damage, as happened in Sweden by their report, an official report this month from one of their government officials, 40 times that this was done. And, they ended up paying extortion. So, you can be hurt on either side.

I would like to use this opportunity, Mr. Chairman, to say, I'm sure to the great relief of the people in the Department of Defense, that I am not speaking for them or for any service. I'm speaking for myself.

But, every statement that I make here is not only unclassified, but I validated it. It isn't just taking rumors or drivel off of the tabloids. These are solid facts that I'm giving you.

Representative Saxton. Okay. Let me just ask a question similar to my question to Dr. Leitner and Mr. Fialka. If this is the situation, what do you see as the remedy?

Mr. Schweitzer. Well, one remedy for your Committee, because of the topic of this morning, in my humble opinion, is to review the export controls, particularly with regard to the critical military list and see if we can't apply to them the same kind of considerations that we give to nuclear technologies.

We are the scientific powerhouse of the world. We produce, develop and are looking into and, in some cases, Senator Bingaman has a constituent in Albuquerque who exports Reltron tubes, which can be used as RF weapons, and certainly will advance the cause of this.

Representative Saxton. Let me just break in again and say, if we can – if I can get into your briefcase and get your book and go down to Radio Shack and buy the components and put one of these devices together, which can be effective in carrying out the destruction that we are talking about, obviously people who are not friendly to the United States can do the same thing.

So, what I was trying to get you to say was you mentioned the notion of shielding electronics equipment and computers in your opening statement. Is that something that we need to pursue as well?

Mr. Schweitzer. Of fielding it, sir?

Representative Saxton. Shielding.

Mr. Schweitzer. Shielding, yes, sir. My keen tanker's ears pick up all these consonants.

(Laughter.)

Yes, absolutely. And, I would defend what was done in the Reltron tubes case. And, I do that in the written statement.

But, we need to take the same low cost technologies and components that we are using to advance the information age in the military and use those same kind of technologies and even components to do the defensive side. That's why I think the people who say that this is going to cost – and one study does say this – the annual defense budget to harden and protect everything, that's really nonsense.

First of all, you wouldn't want to do the whole thing. You wouldn't want to spend that kind of money.

And, you really don't need to. Some of the fixes are low cost, simple and can be applied.

Representative Saxton. Thank you.

Senator Sessions.

OPENING STATEMENT OF SENATOR JEFF SESSIONS

Senator Sessions. Thank you very much, Mr. Chairman. These are very important issues to this nation. And, I appreciate you calling this hearing to discuss it.

It seems to me that we spend a lot of time on a lot of issues that are of marginal importance in the scheme of things. But, the defense of this nation is a core responsibility of this Congress, and we need to give it the highest of attention. And, I appreciate your sharing that with me.

I think back as a poor Civil War historian to the technological developments in the rifle and cannon and it made a difference in that war. I think of John Kiggen's book, "The Face of Battle," talking about at the Battle of the Somme and how many artillery shells were dropped on the Germans. There was only one kind of shell-- and there were very few of them that could penetrate a German bunker. After the artillery barrage was over, the British soldiers were slaughtered on the battlefield.

I think of the Falkland's War. One exocet missile penetrated British defenses and a cruiser was sunk. Today, if some nation of modest power develops a way to penetrate our missile defenses, our whole naval fleet is subject to elimination.

And, I think of the Gulf War. I hope that we are not too overconfident as a result of that war and because of the technology we used to destroy. Those poor Iraqis were just sitting ducks in those tanks. And, that may not be the case in the future if our adversary develops appropriate technology. Maybe our tankers would be in the same position.

We have to be on the cutting edge. And, I don't know how you do that, Mr. Flamm. But, it is absolutely essential to me that we are giving this serious attention.

I am very concerned and really outraged at a suggestion, Dr. Leitner, that the Defense Department would not allow personnel to be here to be considering these issues which are so much more important than some of the others that we spend our time on. I really feel strongly about that.

I saw just this weekend on book notes, an individual who has written a book on the Vietnam War. What that individual said was that civilian leadership, really under President Lyndon Johnson and the Secretary of Defense, kept the military at arm's length and did not allow their honest evaluations to come up through the system. As a result, there were disastrous, strategic consequences in that war that cost thousands of American lives.

I think we need a full discussion of this because it's very, very important to this nation.

And, I would just appreciate, Mr. Chairman, you doing that.

Let me ask you, General Schweitzer, just simply: Is the Defense Department doing enough at this time to defend against these radio frequency weapons?

Is it enough? Just basically just yes or no.

Mr. Schweitzer. It's a painful answer, but a truthful one is no. The fundamental problem is we don't have a strong policy lead. We've got a vacuum there, which is not to say there aren't offices and wonderful people with the title of "Policy" on it.

Somebody has to step forward and say, "This RF threat is only but one of many threats that we deal with. But, we haven't dealt strongly enough with it. We need to focus on it now. And, I will take the lead and advance the cause." That, in my humble judgment, is what is missing.

Senator Sessions. Well, I appreciate that because, as you indicated, it may not be an expensive proposition. But for the want of a nail, the battle was lost sometimes. And, I think we need to think about that.

Furthermore, there are so many situations in which, as you said, Dr. Leitner, a modest improvement in technology can eliminate a whole weapon system. That's what is frightening to me as I think about my responsibility as a senator.

I've not been here but six months, but I don't want it to be written that we allowed some major event to occur that we could have foreseen and that left our soldiers at risk on the battlefield.

Mr. Fialka and Dr. Flamm, I think it's interesting that the "Wall Street Journal" is such a great free market organ of free enterprise and free trade for the world. I consider this to be a very difficult call about

what do you do and what do you allow to be exported; Openness benefits our nation and at the same time it puts us at risk.

Dr. Flamm, you mentioned a third factor in your test concerning the military significance of the technological transfer or openness.

My question is: Are we, in your opinion, operating at the level of sophistication we need to be to make those decisions today?

Is our Defense Department or State Department sufficiently focused on the dangers we face that they can make good decisions?

Mr. Flamm. I would – I will speak to the case of supercomputers and computers, in general, where I have specific knowledge of the decisions that went into that.

In fact, a very real and significant effort was made to actually assess the kinds of capabilities that were linked to exports at different levels of supercomputing power. In particular, given the fact that we had a pretty good idea – in fact, a very conservative idea, as it turned out – of the kind of computing power that was going to be available on the marketplace from foreign competitors of the United States, given that we had actually again a very conservative idea of what was going to be available in terms of older technology that was going to be widely distributed and disseminated, we asked the following question: What military applications of real military significance, that is, using computers, could not be done by taking widely available computers or widely available computers linked together on a computer network, with the application being broken down into parts and run in parallel on the computer network, which is increasingly how these problems are being attacked?

And, we asked ourselves: At what level do we begin to see militarily significant applications that cannot be done by breaking it down into parallel parts, running them on a computer network or on widely available technology?

For the answer we came up with – we had several different sources. There was an IDA study. There was a study done out at Stanford. We had in-house people talking to DOD technical people.

I was working for the technical part of DOD. I represented and worked for the Under Secretary of Defense for Acquisition and Technology.

We went out to the services, talked to people –

Senator Sessions. When was that? What year?

Mr. Flamm. From 1993 to 1995. So, I was -

Senator Sessions. I guess my question is: Do you think it's sufficiently being done today?

Mr. Flamm. I know the right process was used for computers, okay. And, the process was, we went out, we measured what - we assessed what applications could be run - with what was in the market right now, linked together perhaps on networks. And, the break line, the break point was 10,000 MTOPS. That was the first real application that could not be run either on a network or on less powerful computers. And, that's what went into the policy.

Now, sir, you asked what is being done today. The policy today is essentially the policy that came out at the end of 1995.

We are due for a revision. The computer technology, regular as clockwork, has doubled itself again every 18 months. And, we are now in 1997, two years later.

And, it's time to reexamine those limits. And, I suggest to you, sir, to raise them above what can be provided by foreign competitors of U.S. companies, because there is no sense in crippling our own guys and shooting our own industrial base in the foot by preventing them from exporting what is out there in the world market.

So, the fact of the matter is that the controls today were the controls that came out of that rational 1995 process I talked about. And, sir, we are overdue for a reassessment of those controls in a rational way, again applying the same criteria. And, I think we are probably likely - a rational approach to this problem is likely to raise them again.

And, I would only ask -Mr. Leitner's suggestion of a Team B is not a bad one, but I would suggest to you, sir, that it's very important to have people on Team B who know something about industry trends, technology trends and have a good grasp of what is going out in the marketplace. Some of the suggestions for Team B, it seems to me, may not necessarily have that component.

So, I would recommend that you strengthen the Team B approach by seeking out people with specific knowledge of computer technology in the computer industry and where it's going and putting together your Team B.

Senator Sessions. Thank you, Dr. Flamm.

Representative Saxton. The gentleman from California, Mr. Doolittle.

**OPENING STATEMENT OF
REPRESENTATIVE JOHN DOOLITTLE**

Representative Doolittle. Thank you very much. I have found the hearing quite interesting and wish we had more time to learn more about it.

I guess, at least to the reference of computers, Dr. Flamm, your article, "Controlling the Uncontrollable," you don't really believe that we can deal with this problem satisfactorily through export controls and, therefore, you decided - I don't want to put words in your mouth, but I am trying to make sure I understand what you are saying - that it would be better to allow the dominance by our U.S. industries of this global market by allowing the export of their chips; and, in that fashion we would maintain our dominance, because we are able to compete with other countries who are making things that would be able to compete with the chips they are making. Is that right?

Mr. Flamm. I don't think that's a correct characterization of what I'm basically saying in that article. What I am basically saying is that it makes no sense to try to control the \$2,000 or 200 MTOPS computer that you can get in Best Buy that is being shipped, based on chips shipped in the tens of millions units around the globe.

Anybody with basically a soldering gun and a BA, if that, can put together that kind of machine using off-the-shelf technology. That makes no sense to control.

On the other hand, if you are talking about 200,000 MTOPS machines or 600,000 MTOPS machines at the high end of the market, obviously there's a very small number of players who have the capability to put together those kinds of machines. And, those things, you can, indeed, control.

So, I'm saying not let's not control computer technology but let's focus (a) on what you can control, which is always going to be the high end of the market; (b), on stuff that - and focus your resources on what is of real military significance - that is going to make a difference in terms of military capabilities that potential adversaries might have access to.

So, it's not no control. It's sensible controls.

Representative Doolittle. Right. But, with this doubling of power every 18 months, the things that are controlled today in 18 months or three years will not need to be controlled under your view, then?

Mr. Flamm. Some of them will, that's true. Some, not all.

Representative Doolittle. Okay. General Schweitzer, did you want to -

Mr. Schweitzer. Only if you would allow me, sir, to address the chairman and provide perhaps a little deeper answer to his very good question to me.

There are really, sir, two different categories of these weapons. And, there are different ways of categorizing them. I've done that in my paper.

Representative Doolittle. Let me just ask, now you are not talking about computers but we are talking about these RF weapons?

Mr. Schweitzer. Yes, sir.

Representative Doolittle. Okay. Go ahead. Is this on your time?
(Laughter.)

Representative Saxton. Well, if you want, you were pursuing a line. We will get back to RF weapons in just a minute if that's okay.

Representative Doolittle. Okay. Well, Dr. Leitner, do you accept the premise of Dr. Flamm that these things are uncontrollable or not?

Mr. Leitner. In short, absolutely not. The line of reasoning which Dr. Flamm is giving today represents a good deal of what's wrong in the Defense Department today and its attitude towards technology.

The use of empty phrases again, like "uncontrollable," the simple doubling of computer power from one 18-month cycle to the next, so you decontrol everything that went before it, totally ignores the fact of the reality of the computers, how they are used, and the level of computing which pervades the DOD system that exists in U.S. weapons systems. It totally ignores all of this.

Some of the studies that Dr. Flamm has cited were, at best, highly suspect, particularly the one that was commissioned by both the Commerce and Defense Departments. It was done without any anchor into the actual fielded weapon systems in the United States or what we are likely to field in the future.

In addition, earlier, Dr. Flamm stated that the Sandia system is a great example of an easy-to-build, 800,000-MTOPS system. That system that Sandia is trying to build is part of a process that Livermore is engaged in to develop something called the "Accelerated Strategic Computing Initiative," which is an over \$2 billion program, in order to develop that computer.

And, the purpose of the computer is to simulate, in a world that is dominated by a comprehensive test ban treaty, nuclear weapons effects so we won't have to engage in physical testing of nuclear weapons. It's part of the National Ignition Facility, which is being built for Livermore. The two initiatives together run into the billions of dollars in order to simulate nuclear weapons effects.

Now, you don't need computers at that level, 800,000 MTOPS, to simulate nuclear weapons effects. The Russians, according to their own statements, are trying to do it with the computers they just acquired in the 7,000-MTOPS range.

The statements are fairly amusing, because they are totally unanchored to any reality existing in the Defense Department. For instance, current command control and intelligence systems that pervade the Defense Department and that are the backbone of our military intelligence infrastructure have a computational power that ranges from 25 to 2,000 MTOPS. That is what is fielded today.

Even the battle management computationally intensive air traffic control systems - which are used to control and identify up to 1,000 independent targets for air traffic control and for battle management - are in the 1,500-to-2,000-MTOPS range. This is the technology that he advocates simply just flushing away.

Representative Doolittle. But, your belief, then, is that this can be limited and controlled?

Mr. Leitner. Most of the technology in question, whether it's being licensed for production overseas, or whether it's to be manufactured overseas and supplied to middlemen overseas, is almost all of U.S. origin. Almost all the advanced computing technology - if you consider advanced, as over 300 or so MTOPS, is all of U.S. origin.

Under the doctrines and existing laws, like the Foreign Corrupt Practices Act, the U.S. entities operating abroad and their agents are responsible for following U.S. law. So if the same company that is producing chips in Korea decides to sell them to the PRC, it can be held

liable. It should be investigated whether it can be brought to book or the U.S. owner of the technology who awarded that marketing region to the Korean entity. He can't do that in order to circumvent U.S. law.

So, generally the controls can be effective if you cooperate with partners.

When this Administration unilaterally decontrolled computers, it abrogated a bilateral agreement with the Japanese, who are the other main source of supercomputer technology. We simply told them, "We are not interested in the agreement that we had with you for several years. We are simply going to decontrol these things, because it's in our economic interest to do so." And, that's what happened.

What we have here is a marketing argument, not a strategic argument. There was virtually no strategic analysis done of any legitimate nature that underpins the decontrols.

Representative Doolittle. Okay. I have other questions, but I think my time is up. So, thank you, Mr. Chairman.

Representative Saxton. Senator Bennett.

OPENING STATEMENT OF SENATOR ROBERT BENNETT

Senator Bennett. Thank you, Mr. Chairman. I came to learn rather than to question, but I guess the only way I'm going to learn is to ask some dumb questions.

Dr. Flamm, would you like to respond to the response we've just heard?

Mr. Flamm. Yes, thank you. First of all, I would like to - I would like to basically say two things.

First of all, I did not say that the Pentium Pro-based Sandia machine, which is actually about 650, not 800,000 MTOPS, is easy to build, that's something you could do in your garage - that is an example, actually, of what we could control. There is no doubt about it.

So, that's a controllable computer. Don't get me wrong on that.

The second point I wanted to briefly raise is that, in fact, the U.S. is not the only country that can produce the microprocessors that are the component heart. First of all, many of those are shipped under different categories than the computer. It's a different export control problem.

But, more importantly, the U.S. companies are not the only ones that can ship those chips. They are manufactured - microprocessors are

manufactured around the world in places like Taiwan and Korea and Japan and Europe and Israel and many other places.

So, the premise that all we have to do is clamp down on the basic product is wrong – and then there is the whole question of: if you are shipping tens of millions or hundreds of millions of a product, is it really effective to try to export something that is being stamped out like jelly beans rather than focusing on high end technologies that are really linked to serious military capabilities. Those are all the issues that I think you want to ask.

I resent a little bit the implication that I'm speaking for anybody other than myself. I've studied the computer industry for the last 15 years. I know about this stuff. Not everyone knows about this stuff.

And, I would just like to say that what I'm saying today represents the facts as best as I know them and have researched them over the years. And, what I am saying to you is my best rendition of a solid understanding of the industry.

And, I suggest that we want to stick to the facts when we talk about this issue.

Senator Bennett. Mr. Fialka, do you want to get into this?

Mr. Fialka. Yes, thank you. I would just like to add one fact.

My problem with the recent Clinton Administration policy on this and the Brookings Institute approach is that they worship the market, the free market, too much. And, I would –

Senator Bennett. That's an unusual accusation to make about the Clinton Administration.

(Laughter.)

Mr. Fialka. I would point out – not everything that the market does in this area makes sense. I would point you to the fact that the last time we drew the rule, we said, "Okay, you can send supercomputers to Russia, but you can't send them to nuclear facilities."

Now, we have Silicon Graphics, a company that makes supercomputers out on the west coast, sending a supercomputer to Arzamus-16, which is the Russian equivalent of Los Alamos, where they design nuclear weapons. And, after they were caught at it, they said, "Gee, we didn't know what that was."

I would suggest that there needs to be more of a firm hand of government on this whole thing. If American supercomputers are in

highest demand and people that we regard as our competitors or enemies want them, we can, at the very least, slow them down for a while.

Some of our allies, such as Japan, are not going to send them willy-nilly to potential adversaries such as China. I think there is room for common sense on our side of it, too.

Senator Bennett. I think slowing down is probably the only thing we can hope for. I remember the first time I visited the shuttle – bear with me; I am getting to the point here.

I am, like most Americans, in awe of the space program and the technological accomplishment that it represents. I was stunned to discover that the PC I have on my desk that cost about \$2,000 has substantially more computing power than the computers that drive the shuttle.

And the only reason they are not updating the shuttle is that when the shuttle was built 25 years ago, the parts of the computer that drive it had to be wired into the structure so you couldn't take it out without disassembling the whole thing and building yourself a whole new aircraft. Yet, I'm sure at the time the shuttle was designed everybody would have gone ballistic at the thought of giving that kind of computer power information to any potential adversary around the world.

Now they can walk into virtually any shop anywhere in the world and buy computing power substantially greater than we have running the shuttle.

Now, I'm a newcomer to this side of the issue, but I am involved in the whole question of encryption which, I think, is the same issue. The law enforcement people come to us and say, "You cannot allow export of encryption beyond a certain level, because terrorists and rogue states around the world will use that level of encryption to encrypt their messages to each other and we won't be able to intercept those messages and find out who, for example, blew up the World Trade Center. So, Americans cannot export that level of hard encryption technology."

But, you can buy it in America. And, I said to one of the representatives of one of these groups, "A fellow could walk into Egghead Software, buy that hard encryption product, put it on his PC, get on the Internet and, with a stroke of a key, it's available in Libya, Macao, wherever in the world. And, he said, "Yes, but that would be an export and that would be a violation of U.S. law." It may be a violation of U.S. law, but there's absolutely no earthly way in the world to prevent it.

When foreign companies are manufacturing hard encryption products and selling them worldwide and we are prevented from selling ours worldwide, we are doing two things. Number one, we are robbing our country of the export opportunity that is clearly being exploited by other countries, so we are not changing in any sense the capability of foreign nations to have this encryption; and, number two, by not allowing our companies to be in that market, we are hindering their ability to develop new products that could be beneficial to them long term.

And, you know, I'm sorry. I'm a conservative republican who just came from the floor, having attacked the Chinese for exporting C802 missiles to the Iranians and demanding that the Clinton Administration do something about that. I'm going to have an amendment to the foreign relations bill on the floor this afternoon, which I am going to call for a yeas and nays vote on, putting everybody on record and telling Madeline Albright that she is too timid in the way she is handling the Chinese on this issue.

I am no dove on this issue. But, I must say, as I listen to these arguments, I am not persuaded that there is a practical way to prevent the exploitation of this kind of technology around the world.

We can say, "Well, it's a violation of U.S. law." We are like the law enforcement person saying, "It's a violation of U.S. law for him to put that on the Internet."

There is no way in the world you are ever going to find out who did it or prevent it. And you might as well recognize that.

Now, with that kind of a speech, does anyone want to react violently one way or the other?

Dr. Flamm? And, I apologize, Mr. Chairman, for going over.

Mr. Flamm. Is a not totally violent reaction appropriate?

Senator Bennett. Whatever.

Mr. Flamm. I guess I want to say two things. It's a similar issue, at first glance - by the way, I'm in the process - there is going to be a - Brookings is putting out an encryption policy paper that I wrote shortly. So, the -

Senator Bennett. Send me a copy.

Mr. Flamm. I will. You will get one. I would suggest to you that encryption is somewhat different than computers for three reasons.

First of all, in many respects, it's a smaller group of players. The people who can do sophisticated encryption software that is really quality controlled is probably smaller than the people who can buy a motherboard, a computer chip and slap together, you know, a Best Buy, low end PC, number one. The technology is more closely held.

Secondly, there's one big difference between an encryption package or encryption hardware even and a computer. And, that is, a computer, the user can evaluate and judge how good it is. If you want to know whether the new PC is going to give you a lot of benefit, you can buy the thing or you can borrow it, you can run your applications and you have a pretty good understanding of how good that computer is for your purposes.

Encryption technology is different – the trick in encryption technology is it has to defend against the other guy. You can run it until you are blue in the face and poke sticks into it, and you are not going to necessarily know if a sophisticated opponent can take that thing apart.

So, that's a subtle but important difference between a computer and encryption technology.

And, finally, in some respects – there are other issues involved as well, because we have been talking about national security and economics here today when we've been discussing computer exports. And, there are other issues that come in with encryption as well – privacy issues, civil liberties issues – important issues that need to be talked about that I think are not quite so intertwined with the issues that we are talking about here today with computers.

So, I also think it's a very difficult problem. I think there is some irony, as you say, sir, that on the one hand the Clinton guys are getting clubbed over the head for being too liberal on computers and they are getting clubbed over the head for not being liberal enough on encryption.

I agree there are some ironies or paradoxes in this situation. And, I'm not sure what the proper balance is. But, I can assure you, they are sweating a lot about it, when I talk to people in the Administration.

Senator Bennett. Thank you.

Representative Saxton. Mr. Doolittle.

Representative Doolittle. Thank you, Mr. Chairman. General Schweitzer, now going to RF for a minute, was it the application of RF, what we did to disable Iraq's capabilities in Desert Storm?

Mr. Schweitzer. I would rather defer a clear answer to that to another type of hearing, sir, on what we actually did in that area.

Representative Doolittle. Well, I guess I'm just trying to ascertain if that's the sort of thing we are talking about when we say RF -

Mr. Schweitzer. Radio frequency weapons that would neutralize the electronic gear. And, it was brought out earlier from your side of this discussion that a future enemy could do this very readily to us.

And, that is really the point I would like to clarify with the Chairman, if I may.

Representative Doolittle. Sure, go ahead and clarify it.

Mr. Schweitzer. First of all, and maybe the best way to do this is to say that - because so much of this discussion has properly focused on China - China this past month announced from the Navy Research Institute, their director of R&D, that they were going to procure three types of RF weapons - one which would attach the electronics, one which would be beams for precision strike and another electromagnetic pulse systems, which would give them a capability for plasma weapons. This we haven't gotten into on all the arcane details and scientific details of this. That's why the -

Representative Saxton. General, you just used a term that is not familiar to many of us - plasma weapons. Would you explain what that is?

Mr. Schweitzer. Well, what you do with an RF weapon, very simply stated, sir, is you put out a wave of energy, which is a plasma wave breaking through the air. And, it's this way that the power gets to the target.

One of the interesting things about this is that when you look at these weapons, they are not all replicated by going to some commercial off-the-shelf catalog or Radio Shack. They are an entirely different degree.

Everything depends on pulse strength, pulse duration, rise time, which gets the power up. These are the critical factors.

And, the things that you can get commercially off-the-shelf that would affect the infrastructure are one thing. They are primitive devices.

But, there are major weapons that can shut down the amphibious force, that can stop the C-41s from delivering troops to a theater, that can knock down all of the command and control, your artillery, your radar,

all your systems that have electronics. And, these bigger weapons, which we are capable of developing.

And, as the scientific powerhouse and the leader, really, in this entire field, when we send these devices overseas to countries that are now friendly but who, themselves, have no technology or transfer controls will just sell to the first and best and highest bidder. That's my concern.

And, that's what I don't think I clearly enough stated in response to Chairman Saxton's question to me, because I wouldn't want the Committee to leave thinking that we don't need export controls and to have them review - for example, RF components are on the military critical technologies list. But, there has been no policy or direction on these for about two years.

And, two years ago - maybe it was three - when the regulations were written, the directives were written, not much was known about them. And, they weren't very clear. And, they are not working very well. And, they are confusing the scientific community which is then left to make the recommendations to the State Department, should we or should we not go along with this particular transfer.

And, I speak to that in the written testimony in some detail.

But, as long as the distinction is clear, we want - and I think this Committee would want - RF components to be looked at for the major systems, the major weapons that can do real harm even to the infrastructure, to be looked at the same way that we look at nuclear technologies, which is done very carefully. And, the direction and guidance on that is very clear because, of course, we've had that problem with us for a long time.

I think that one of the things that helps you realize this perhaps a little better is in the written testimony but not possible to explain in the oral statement. There's another group of these weapons, if you will - hand grenades, mortar rounds, artillery rounds and missiles - where an explosive-driven device provides the initial burst of energy to set the rise and the pulse and get the power up there.

In other words, if you think of a hand grenade - and there is such a thing that the Russians have - it's propelled, a rocket-propelled grenade, over the fence at the White House at the OEOB, it goes off, there's a little explosion noise and a little damage from the fragmentation of the casing, but that's not the primary effect. An antenna, a little antenna, comes up

and then the wave is propagated and now the power is projected, either a narrow beam or an ultra wide beam, to affect the innards of the electronic components inside the building. And, it would shut down the operation there.

So, here is a weapon, a use of the weapon, which would be very appealing to special forces type units, to people who want to do this covertly. The people who would use these weapons are criminals, mentally unstable people, terrorists, narco traffic kanter.

And, that is more of the context in which I was responding to Chairman Saxton's question when he raised it to me.

But, if you have an adversary, a nation, large or small, or a group representing itself and using the funds of a nation, a semi-religious group violating every tenant of their religion in so doing but operating under that cover or cloak in some small nation or a large nation, that then wants to inflict great, serious, major harm on the United States, now they use a larger weapon, the components of which they got from us or through the technology transfers or sales of equipment to friendly countries who then, in a heartbeat, would sell these to others. I think China is getting its technology - in this case, they are seeking obviously to get it from Russia. But, Russia - and it's important to know this - even in the development of the weapons they have, they relied heavily on the expertise of our great scientists going back to the late 1940s.

But, I think that there is a problem at the higher end of this spectrum, if you will, to look at the export controls for RF components in a reasonable way. We don't want to shut down or cut ourselves off from contact with a whole segment of what is happening in science. And, I talk about that in the paper.

On the other hand, the Chairman's point, of course, is exactly correct. Indeed, it was mine, that you can go to the commercial off-the-shelf side to get primitive devices that can still inflict great harm.

But, it doesn't mean - it's not an either/or situation. You could have an adversary - and that's what I'm concerned about - an organized, determined, well-financed adversary who hates us, who would get these major weapons and use them against the national power grid, the national telecommunications system, the national transportation system and shut us down.

You know, a lot of this goes back to our use and our knowledge of nuclear weapons. If an adversary were ever to get hold of one of those

things today – and that's why the nuclear threat is so seriously addressed in the Quadrennial Defense Review and in a lot of your discussions and in other committees, and it needs to be, because a nuclear weapon detonated 400 kilometers over Kansas out of a satellite should Saddam Hussein or somebody like, Mr. Quaddafi and Libya, ever got hold of one of these or somebody in Iran and decides to use it against us, there isn't any signature from that because it's dispensed by the satellite. And, at 400 kilometers over Kansas, it would have a continental effect on the United States.

Everything that I've talked about – the vulnerabilities, the targets – you would shut it all down, telecommunications, power grids. Even the railroad lines in that case become antenna as the electrons come down. The entire railroad line would act to conduct what you are sending down.

So, I think that while we want to look at the standpoint of protecting the infrastructure which, I say, is immediately a threat from the off-the-shelf devices, we also want to look into the future, as you have been doing here, and provide protection for the more powerful devices that can be exported and transferred that would be used against us by adversaries in the future. And, that's why the policy lead is so important.

And, I do want to say that there is nobody in the Defense Department that is doing anything wrong. They have been preoccupied with all kinds of other problems. The RF threat is only one.

This has stayed bottled up for a long time, and it's just now coming to light. And, that's why this hearing is so important and any future ones, sir, that you care to hold.

And, I would be happy to give you the names of the real experts on this who can talk – who have worked on this for many years. And, I think it's important that we do that. Our focus should be on the immediate danger, in my mind, which is the threat to the economic infrastructure, which we can't even define at this point. What is it? It's an amorphous term. What in it is susceptible and vulnerable?

Representative Doolittle. Is it possible – do we have technology to allow, say, the Dirksen Building to shield itself from the van driving around emitting those pulses?

Mr. Schweitzer. Yes, sir. You can – there are many ways to protect, and there are many vulnerabilities on it. And, we just have to get a good start by beginning to scope the problem, by getting the right people in.

And, incidentally - Senator Bingaman is no longer here. But, these are the last words. And, I would not want to leave this hearing having left behind a suggestion that what we need is another study for the offensive weapons that need to be developed.

That knowledge and technology is well in hand. All it has to do is be modestly and moderately and properly funded. And, Los Alamos and Sandia, Livermore, the great national labs, can deliver.

And, these are other arrows in the quiver. They don't substitute for the armed forces that we have now.

War is a matter of action and reaction. And, there will be other things that will come along.

The greatest folly would be to say, "Well, the RF weapons will replace forces," that, in my humble opinion, we don't have enough of.

But, at the other end, the protection of the infrastructure - because that's what is threatened now - that's something we ought to start working on. And, there's plenty of talent, there's plenty of ability and there are a number of people who can take the necessary policy lead.

Thank you, sir.

Representative Saxton. Thank you, General Schweitzer. Let me ask a question of Dr. Leitner and Mr. Fialka.

Dr. Leitner, you mentioned some rather immediate threats to the transfer of technology that are opposed by some activities, as did Mr. Fialka, currently being carried out by the Chinese government or arms thereof, alleged arms thereof. One such activity is involved in the shipping industry, particularly with a firm known as COSCO which, as you pointed out in your testimony, currently controls a shipping port or facility at either end of the Panama Canal, as well as apparently ownership or the lease of one in Long Beach, as well as regular ports of visit in various places around the United States.

Would you care to (a) suggest who it is that owns COSCO, which has been portrayed as a private company, a private firm, and the impact, the potential impact, you see of this company's activities with regard to the subject we are discussing?

Mr. Leitner. To the best of my knowledge, COSCO is an arm of the Chinese government and is also affiliated very closely with the PLA and is used as a primary logistics arm.

Representative Saxton. Excuse me for interrupting. It has been said fairly consistently by some that it is a private company.

And, what is its connection to the PLA, if that is so?

Mr. Leitner. For a direct connection to the PLA, you will have to invite somebody who is a real China expert who monitors the infrastructure and the various facilities in China, which I can't speak to at present.

The concept of private ownership in China is a different concept from private ownership here. It's like people saying that CATIC, that Mr. Fialka referred to, which bought up these aerospace facilities from the United States, is a private Chinese company. It's not. It's an arm of the government that is directly controlled by one of the ministries and departments of the government. They all work hand in glove with the People's Liberation Army, Navy or Air Force, and they work towards a common purpose that is centrally directed.

They may have some local autonomy when they operate overseas and under the laws of a particular country to operate as an ongoing business. But, they are centrally directed by the Chinese government. And, that's true of most businesses in China.

Representative Saxton. Okay. Then, let's go on to (b) and suggest what it is that may be of concern to us relative to their various locations, particularly in the western hemisphere.

Mr. Leitner. Well, other events have taken place recently, too. I believe President Clinton signed a treaty or an agreement within the last year or so allowing the Chinese to have greater access to U.S. ports all over the place, including a major naval base such as Norfolk, Bremerton in Washington or San Diego, basically allowing them to come in with some minimal prior notice and simply embark or disembark whatever they want to in those locations. They can come into the port with COSCO ships.

Now, if I were a suspicious type, which, of course, I'm not, and if we were concerned that the Chinese might misuse this as part of some sort of military collection activity, which they are well known to do, or even, say the General talks about the RF weapons and how they can be used to disrupt infrastructure, think for a minute what a Chinese-flagged LNG tanker, a liquified natural gas tanker, can do to the port of Norfolk, an entire military base at Norfolk, the world's largest military facility. If the spigots are open and the gas is atomized in the atmosphere and an

incendiary device is used, you can level the entire facility and the U.S. Atlantic Fleet with it.

So, how much access you really want the Chinese to have at U.S. military facilities – absolutely critical facilities that are the lifeblood of this country in our ability to remain independent to conduct an independent foreign policy and protect our nation— is quite problematic. So far, there hasn't been any real exploration of it that I've seen. But, it has tremendous potential consequences.

Representative Saxton. In your testimony, Dr. Leitner, you also mentioned – and had a chart up of – George Air Force Base.

Mr. Leitner. Yes, sir.

Representative Saxton. This is the chart. George Air Force Base, which is in California, is a base that was closed by our – through our base realignment process; is that correct?

Mr. Leitner. Yes.

Representative Saxton. And, at George Air Force Base, you must have some information that suggests that the Chinese are doing something there which could also be detrimental; is that correct?

Mr. Leitner. Yes. Right now, it's very preliminary.

But, there is a real potential for a PRC intelligence operation – and usually under the cloak of business there comes some sort of intelligence capability as well – right within a couple of blocks of George Air Force Base. Now, the air force base itself is no longer an air force base. I think it's called the Southern California International Airport, and it's being commercialized.

Representative Saxton. Have American taxpayers turned over some facilities to the Chinese interests here?

Mr. Leitner. Not that I'm aware of on the facility itself. I understand, from doing searches on Internet, that the Chinese have been negotiating for the purchase of a very large tract of land for an industrial application next door to this facility. And, whether there are any government subsidies involved in that land transaction, I don't know. It's possible, but I just don't know at this time.

Representative Saxton. So, I guess the point is that George Air Force Base is currently used for a variety of other purposes which the Chinese would like to snuggle up next to, in your opinion?

Mr. Leitner. Particularly the development and the manufacture of the Predator RPV. But one of the most interesting things about why U.S. military facilities are located where they are facilities is there is some politics to it as to where you would build your bases. What this chart attempts to show is the absolutely strategic location in a neighborhood of the most advanced research and development for aerospace and stealth technologies that the U.S. has.

Representative Saxton. Let me make sure I understand, that we all understand, that your concern is that the manufacturing facility may be used for other purposes other than for manufacturing facilities; and, there is a record to support that that notion is one that ought to be taken seriously.

Mr. Leitner. Yes, sir. By installing an array of antennas in a false roof of these 30,000-or 40,000-square-foot retail facilities or warehouses, the Chinese can intercept a good deal of the telemetry coming back from the Pacific Test Range. Very often the telemetry conducted in tests in the United States is not even encrypted for military tests.

Representative Saxton. So, the notion here that this chart portrays graphically is that Nellis Air Force Base, which is the headquarters of our Strategic Air Command which is no longer called the Strategic Air Command - but essentially that function is still carried out there, correct?

Mr. Leitner. Yes, I believe so.

Representative Saxton. Yuma Proving Grounds is also a few hours drive from there. The Marine Corps Air Ground Combat Center is within a two hour drive from there.

Marsh Air Force Base is within a one hour drive from there. Norton Air Force Base is close by.

The Northrop-Grumman plant is close by. The McDonnell Douglas plant is close by.

Edwards Air Force Base, which is the aerospace test center, is close by. And, so the concern that you raise is that (a) there is a presence there of a concern that you believe may be of concern relative to information-gathering and other acts of technology transfer -

Mr. Leitner. Espionage, sure. Looking at the facility location, the physical location, it's an ideal location, you know, for a collection effort.

The concern is: Is anybody, the F.B.I. or anybody, looking at the establishment of a foreign presence at locations which are obviously as

strategically located as this one is. It's high desert; it's over 2,800 feet, I believe, in elevation. It's an ideal place for gathering intelligence, particularly for intercepting what is in the airwaves.

Representative Saxton. Mr. Fialka, let me just turn to you for a moment, because you made a brief mention of a lucrative subject. A kind of headline of your discussion may have been lucrative business deals provide an opportunity for technology transfer and espionage.

You talked about one in particular that had to do with the transfer of some high technology machinery of some kind along with apparently an aircraft deal.

Dr. Fialka. This was Plant 85 in Columbus, Ohio. It is a plant that has made many things.

It's what is known in the Pentagon lingo as a GOCO, a government-owned company operated.

Representative Saxton. That's GOGO?

Dr. Fialka. GOCO.

Representative Saxton. GOCO?

Dr. Fialka. Yes. And, over time, it has made cruise missiles, the skin for the Titan missile, the new transport. It has done a lot of high tech things for the U.S. Air Force.

And, all of a sudden, we see these machines going to China. These are computer-driven lathes and milling machines. Some of them are the size of this hearing room.

They are very exotic. They involve a lot of taxpayers' money. And, they can do many, many things.

And, as I tried to describe, they were squeezed out of us in a so-called business deal. But, as Dr. Leitner is pointing out, a lot of these aren't really just business deals. You are dealing with a potential military adversary who thinks both business and commercial at the same time.

One of the things that hasn't been discussed here is the access they have to our markets in all sorts of items. There are over 100 branches of the PLA, the People's Liberation Army, that sell commercial goods in Wal-Marts and K-Marts.

And, I am talking about simple things like automobile jacks and teddy bears and oak toilet seats. People have no idea. They think they

are dealing with Chinese companies that just happen to undersell the market.

This money goes to the People's Liberation Army.

Representative Saxton. Okay. We have just outlined in the last couple of minutes three different instances where there is a potential leak of transfer from our side to the Chinese side - COSCO, George Air Force Base and lucrative business deals.

Now, does the federal government have any role in controlling these activities?

With regard to COSCO, Mr. Leitner, was there or is there a federal role in approving or disapproving, permitting or not permitting, the operations of COSCO?

Mr. Leitner. If you are referring to COSCO at the Long Beach facility, I am not sure. The federal role should be one of vigilance; and, certainly for counterintelligence, the F.B.I. should be involved.

Representative Saxton. Did you not mention that the Administration approved some activities for COSCO which have recently come to pass that permitted them to use ports in various parts of the country that apparently weren't possible before?

Mr. Leitner. There was recently, to my knowledge, a treaty or an agreement signed which gave the Chinese greater access to U.S. ports. I am not sure if it was a Freedom Commerce and Navigation Treaty or what the technical terms of the treaty were, but they gave the Chinese enhanced access to U.S. ports, yes, including our key military ports as well.

Representative Saxton. Now, with regard to the situation at George Air Force Base, obviously you are concerned, and we are concerned or we wouldn't have had this hearing today. Is there a federal role in determining what types of activities go on in this free enterprise, Chinese factory, et cetera, whatever other activities are carried out there?

Do we have a role there?

Mr. Leitner. Once the deal is established and a "wholesale outlet" opens up where they are selling goods from a particular country, when they are operating within the U.S. borders and have a company that will hire some local citizens and they will create some employment locally in the economy and be welcomed with open arms, there are no restrictions on their operations once they are internal to these borders. The only

thing you can do at that point is if you have suspicions that it's an intelligence operation or some technology acquisition operation that is going on, then it's the province of the F.B.I., to my knowledge.

Representative Saxton. To your knowledge, is our government looking at that issue?

Mr. Leitner. To my knowledge, I have no indication at all that anybody is looking at the issue. As far as I know, this is the first time this issue is being discussed.

Representative Saxton. And, Mr. Fialka, with regard to various business deals with defense contractors, does our government, have a responsibility, in your opinion, to monitor those deals or even approve those deals?

And, was the deal that you made reference to subject to any federal approvals or monitoring?

Mr. Fialka. Oh, yes, it was. It was approved by the Department of Commerce with input from everybody. DOD happened to override its own experts.

Basically, you have two scenarios. China could come to us and say, "We want to buy this exotic machine that once made cruise missile skins and other things." And, the straight up and down answer would be, "No, that's a weapons technology. You can't have it." That's probably what the Commerce Department would say.

But, when you get McDonnell Douglas to go in and say, "Gee, we are in the middle of this billion dollar deal and couldn't you be nice just this once and let them have these old machines, because then we get this billion dollar aircraft deal," that swings the politics in a different direction. And, in this case, it looks like the Clinton Administration said, "Hey, we have a \$30 billion trade deficit. This is a billion dollar deal. Let's do it."

Well, now the trade deficit is up to \$45 billion or thereabouts. I suppose we could do two more deals like this if we wanted to.

I guess my argument is we can't afford it. And, I guess what I would like to see - this is a black box over at the Commerce Department. We have no idea what arguments go on over there. I would like to see more transparency so that when a McDonnell Douglas decides to do something like this more people know about it.

Representative Saxton. Well, thank you very much. I have no further questions.

John, would you – do you have other territory that you would like to cover here?

Representative Doolittle. Briefly, just one thing we didn't touch upon. Our so-called friends, the Russians, weren't they the ones at Bremerton who were firing the laser weapon at the pilots' eyes? And, this happened just – I don't know when it happened, but it was reported, I think, within the last couple of weeks.

Mr. Leitner. Yes, sir. That was reported widely in the press that it happened off of Bremerton, I believe, and it was a navy aircraft. I believe that's what it was.

And, it's not the first incident either. It has happened before.

That's why I bring up, in part, the issue of the laser blinding weapons, which are included in my presentation. Like General Schweitzer's RF weapons, these are a very devastating sort of a weapon for which there is a very, very expensive cure. They can have a very great impact on our current investment in military technology.

For one point, it can simply eliminate the manned aircraft from the loop, because in order to defend against a wide variety of laser frequencies, which can be shifted easily, there are big U.S. programs to develop an agile laser that can shift from one part of the frequency spectrum to another. There's a very, very difficult problem in trying to defend against it. You can have goggles that are wave-band-specific that can eliminate a particular wavelength.

But, when you are able to shift them at random, almost instantaneously, or use a variety of lasers concurrently, all operating at a different part of the frequency, it's impossible to defend against. And, unfortunately, the sensors aboard the planes are equally as vulnerable as the human eye.

Representative Doolittle. Is this something, this hand-held thing, is this – it's aimed like a rifle or something?

Mr. Leitner. Some are. The companies like McDonnell Douglas have developed a rifle system called the Cobra, which is basically mounted on an M-16 frame, the stock of an M-16.

There are other competitors, too, that have developed these things domestically. And, they operate on batteries.

I believe one of the systems had about a billion rounds per recharge, that you can squeeze off about a billion rounds. If you hold the trigger down, you have a steady beam. Of course, you have fewer rounds, but you get a billion per charge. And, that's from the initial prototype.

The Chinese, unfortunately, in the last couple of years have been trying to sell laser blinding weapons at some international trade fairs. And, one looks like an M-60 machine gun, which they have been actually actively trying to market. They have brochures on it, and they have been giving them out all over the place. It is for anti-personnel and anti-sensor applications.

Representative Doolittle. Thank you.

Representative Saxton. Dr. Leitner, you made a statement at the close of your opening statement that sounded like - certain members, certain colleagues of yours were discouraged or prohibited from coming here today.

Mr. Leitner. Yes, sir.

Representative Saxton. Were you discouraged from coming here to talk with us?

Mr. Leitner. Well, my testimony was cleared by DOD with much chagrin, but it was cleared, which is a testament to the openness of the Defense Department on this issue. That's pretty remarkable.

My leave slip was never signed off on. I put in for annual leave.

I was told I can't take administrative leave, so I'm doing this on my free time. So, I'm doing this as a private citizen, which is appropriate.

But, I was not prevented, no.

Representative Saxton. Was there some concern about the subject matter in terms of classified sensitivity?

Mr. Leitner. No, sir. The testimony, again, was cleared and had a pretty rigorous review within the Department. And, there were no issues of security or anything else.

There was one change that was made. But, that's basically to ensure that it's clear that I'm speaking as a private citizen and the author of a couple of books as opposed to a representative of the Defense Department.

Representative Saxton. Well, there obviously was some concern about the information that you might give us today. And, I guess my

questions are going towards trying to find out what that concern – why that concern was there and whether – obviously people feel strongly about it, because they went to file apparently some kind of a civil suit because of the actions that were taken by the Department of Defense.

Mr. Leitner. Well, not a civil suit. They filed a complaint with the Inspector General's Office that they were being barred from exercising what one might consider a constitutional right of attending an open hearing of the government and using annual leave for that purpose, even on their own time.

Representative Saxton. Do you know why?

Mr. Leitner. It's hard to judge why. You could surmise that they are afraid. It's possible that there is some sort of fear that people might coalesce into an organized opposition or whatever.

I really don't know why. I can't read other people's minds.

Representative Saxton. All right. Well, I won't push the point any further. But, it obviously is something that would concern the Committee members.

I would like to thank each of you for being here today and my colleagues who stayed here for almost two and a half hours. And, obviously a lot of things have been brought to light today which are extremely important – RF weapons along with the other issues that we've been talking about.

One of the things that the Joint Economic Committee does, as a matter of practice, is to make information that we cover available to other Members. And, General Schweitzer, I can assure you that the Chairman of the R&D Subcommittee on the National Security Committee on the House side will have full and immediate access to the issues that you've talked about, as well as others here, others who may be interested in the Congress.

So, thank you very much for being with us today. You have all been very helpful. And, we will look forward to seeing you all again.

Thank you very much.

[Whereupon, the hearing is adjourned at 12:26 p.m., Tuesday, June 17, 1997.]

SUBMISSIONS FOR THE RECORD

PREPARED STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

Ladies and gentlemen, 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, *Reforming the 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 Kenneth 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 for Dual Use technology Policy. At Brookings, Mr.

Flamm has focused much of his research on international competition in high technology industries.

Let me add one 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.

Testimony of
Dr. Peter M. Leitner
before the Joint Economic Committee
of the United States Congress

June 17, 1997
10:00 a.m.

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.

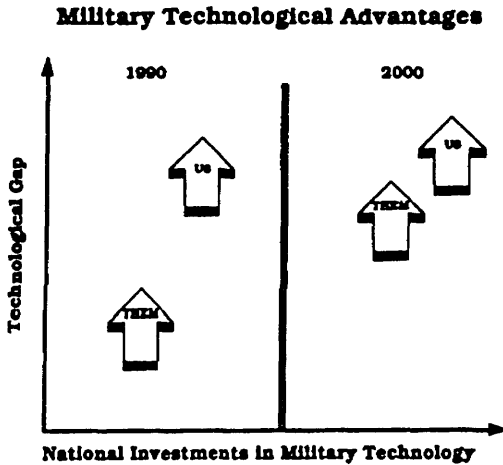
Threats to U.S. National Security

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."¹²

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



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."⁶

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 $1 m^2$ 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 of computers 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 10, 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

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

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

³Larry 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)

⁴The most critical feature is the expression:

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

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.

⁵Michael Borus 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.

⁶Ibid., 123.

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

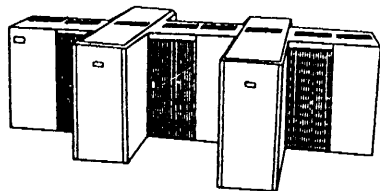
⁸*Ibid.*, 1.

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

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

ATTACHMENT A

HIGH PERFORMANCE COMPUTERS



The decontrol of all computers below the 500-CTP threshold would suddenly make available to any proliferant state-of-the-art CAD/CAM or signal-processing workstations that are more capable than anything in the US defense sector. An example of the strategic importance of such access can readily be seen in the aerospace/missile development field. High-speed, ultra-precise, and graphic-intensive workstations employing advanced (but recently decontrolled) software such as Computational Fluid Dynamics or Finite Element Analysis would obviate the need for expensive, thermally conditioned, wind tunnel facilities. The ability to rapidly model and alter size, shape, density and material characteristics in three dimensions and real time is what these workstations were designed for. A proliferant country could then totally conceal its R&D efforts for, say, ballistic or cruise missiles until it has developed a flyable prototype. Workstations at this level also play a pivotal role in the design and development of microprocessors, integrated circuits, dense memory, etc., thus providing the critical enabling technology for indigenous commercial and military devices.

A severe impact would also occur in the areas of ASW, STEALTH, C³I, C⁴I, Tactical Weather Forecasting, Nuclear, Chemical, Biological weapons development as well as each of the 21 critical military technologies identified in the DoD Critical Technologies Plan (see below). This impact is directly related to the computational, memory, speed, storage, networkability, communications, and graphics performance of systems in the range decontrolled.

STRATEGIC IMPACT

An analysis of the technology embodied in the North American Aerospace Defense Command (NORAD) reveals that the continual erosion of export controls has resulted in the decontrol of virtually every system or sub-system at the heart of this nation's strategic and ballistic missile defense capability. Examples include:

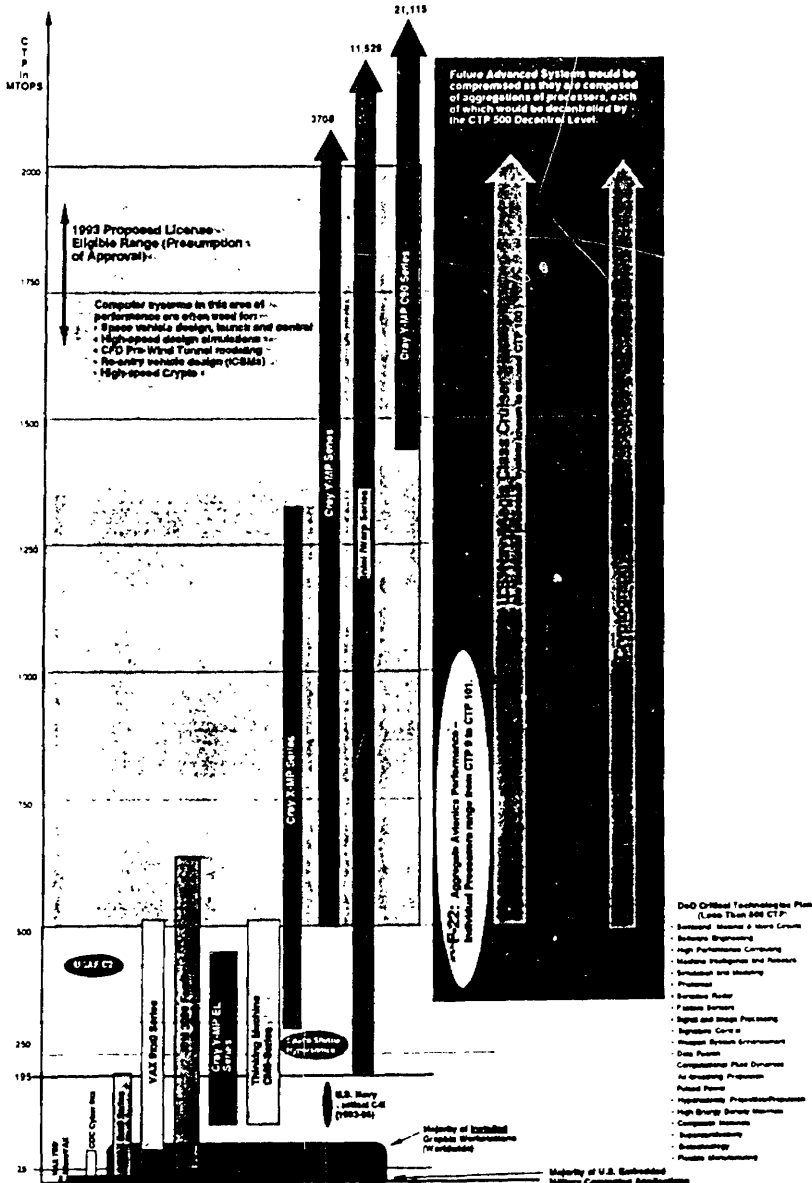
- Fiber Optic Communication systems and Cables
- Large format tactical displays
- Computers and Workstations
- Advanced communications and encryption devices
- Advanced Radars
- Advanced Signal Processing Systems

NORAD has just brought up to operational status an upgraded computer system to receive and integrate data from its region and sector operations control centers. This \$10 million system consists of two types of Hewlett-Packard computers rated at 189 and 99 - 300 MTOPs respectively. This newly decontrolled system is illustrative of the strategic applications which will quickly be made available to potential adversaries.

The decontrol of such powerful computing/analytical platforms obviates the need for large computing facilities or mainframe supercomputers such as a CRAY for weapons design, testing or command and control. Coupled with the recent and anticipated relaxations in the area of telecommunications, this makes rapidly relocatable and survivable C³I possible and testing of advanced weapons highly portable, concealable and inexpensive.

The 21 Critical Technology areas:

- Semiconductor Materials and Micro Circuits
- Software Engineering
- High Performance Computing
- Machine Intelligence and Robotics
- Simulation and Modeling
- Photonics
- Sensitive Radar
- Passive Sensors
- Signal and Image Processing
- Signature Control
- Weapon System Enhancement
- Data Fusion
- Computational Fluid Dynamics
- Air-breathing Propulsion
- Pulsed Power
- Hypervelocity Projectiles and Propulsion
- High Energy Density Materials
- Composite Materials
- Superconductivity
- Biotechnology
- Flexible Manufacturing



CTP Ranges of Computer Systems Used for High-end Computing Applications (1975-1992) Such as Computational Fluid Dynamics, Weather, Sound Analysis, High-performance Jet Engine Design, etc. and Some Advanced Military Weapons Systems

- DoD Critical Technologies Plan (Less Than 600 CTP)**
- Satellite Control & Mission Control
 - Defense Engineering
 - High Performance Computing
 - Mobile Intelligence and Research
 - Simulation and Modeling
 - Procedural
 - Simulation Power
 - Processors
 - Signal and Image Processing
 - Software Core
 - Proposed System Environment
 - Data Fusion
 - Computational Fluid Dynamics
 - Air Modeling Processes
 - Power Plant
 - Hydrodynamic Processes/Processes
 - High Energy Source Machines
 - Composites Systems
 - Instrumentation
 - Acoustics
 - Physics Simulation

Majority of U.S. Estimated Military Computing Applications (i.e., Cruise Missiles, Network...)

ATTACHMENT B

MAJOR PUBLIC AUCTION

MAJOR CNC 5 AXIS MACHINING & FABRICATING FACILITY

MACHINERY & EQUIPMENT

NO LONGER REQUIRED FOR CONTINUED OPERATION

NORTHROP GRUMMAN**\$2 MILLION
EVALUATION****B-2 DIVISION****8900 EAST WASHINGTON BLVD
PICO RIVERA (LOS ANGELES) CALIFORNIA****WEDNESDAY, AUGUST 23, 11:00 AM****INSPECTION: TUESDAY, AUGUST 22****8:00 AM TO 3:00 PM**

REGISTRANTS FOR INSPECTION & AUCTION MUST COMPLY WITH TERMS ON PAGE 7

**INDUSTRIAL ASSETS, INC.**WESTERN CORPORATE OFFICE
11425 VENTURA BOULEVARD, SECOND FLOOR
STUDIO CITY, CA 91604
(INSIDE CA) 818-508-7036 • FAX 818-508-3025TOLL FREE
(OUTSIDE CALIFORNIA)
800-243-4887EASTERN OFFICE ADDRESS
CROWN CENTER BUILDING, 2101 SANDS RD. N.
SUITE 204, BOX 20, CHARLOTTE, NC 28227
704-861-1334 • FAX 704-845-6332

LIQUIDATION SALE

Machinery & Equipment no longer required
in the continuing operations of

**Lockheed Martin
Aeronautics Division**
Littleton, Colorado



**NORMAN LEVY
ASSOCIATES, INC.**

Auctioneers / Liquidators / Appraisers

Headquarters: Southfield, Michigan

Offices in: Boston, Massachusetts • Chicago, Illinois
San Francisco, California • Coventry, England

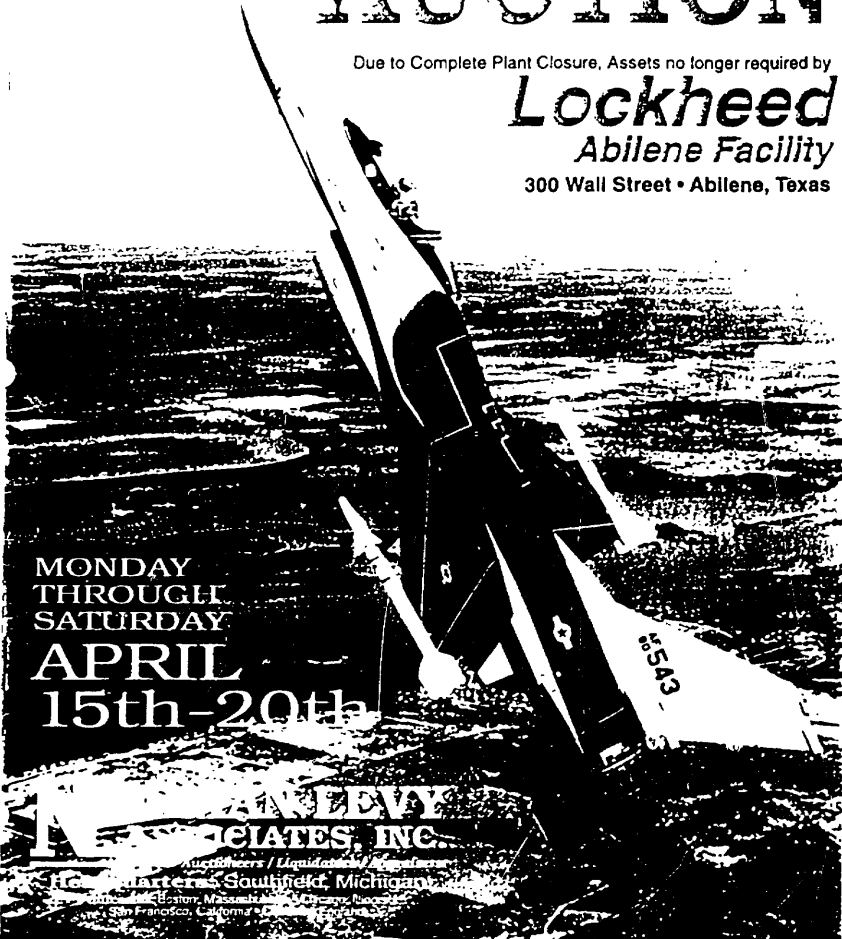
6-DAY PUBLIC AUCTION

Due to Complete Plant Closure, Assets no longer required by

Lockheed

Abilene Facility

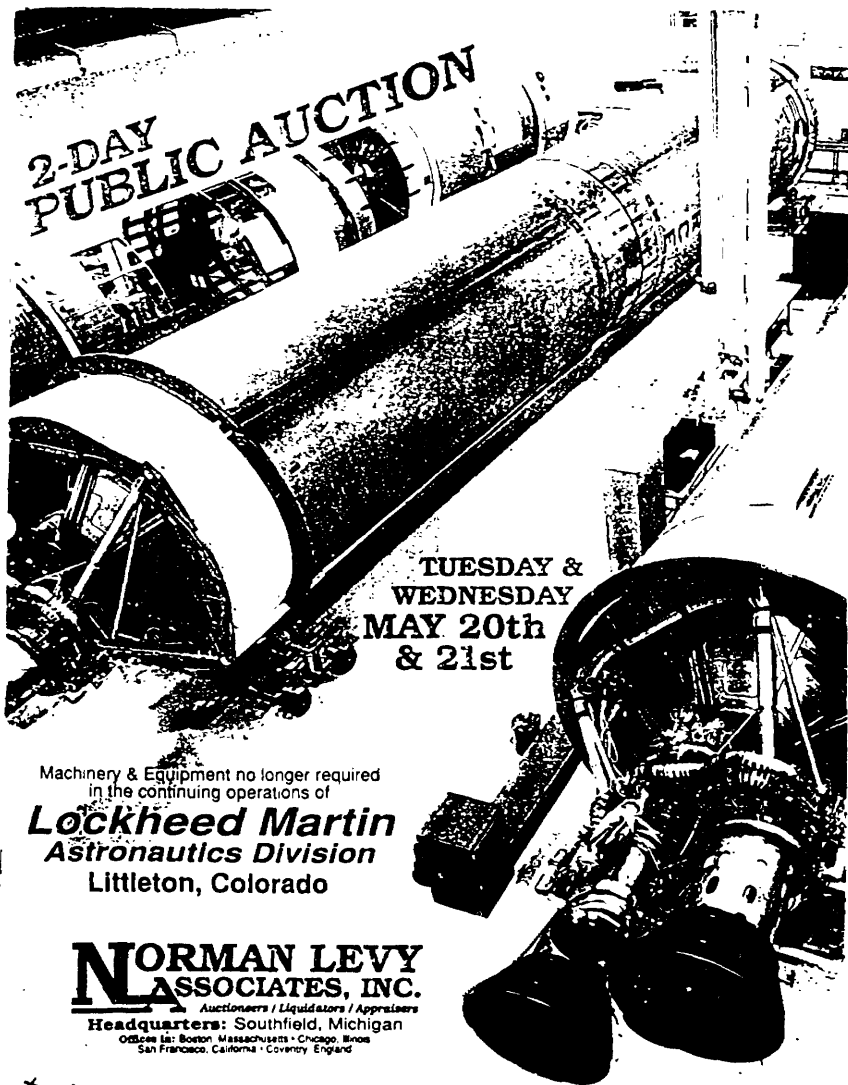
300 Wall Street • Abilene, Texas



MONDAY
THROUGH
SATURDAY
APRIL
15th-20th

**NEWMAN LEVY
ASSOCIATES, INC.**

Headquarters: Southfield, Michigan
Branches: Boston, Massachusetts • Chicago, Illinois
San Francisco, California



**2-DAY
PUBLIC AUCTION**

**TUESDAY &
WEDNESDAY
MAY 20th
& 21st**

Machinery & Equipment no longer required
in the continuing operations of

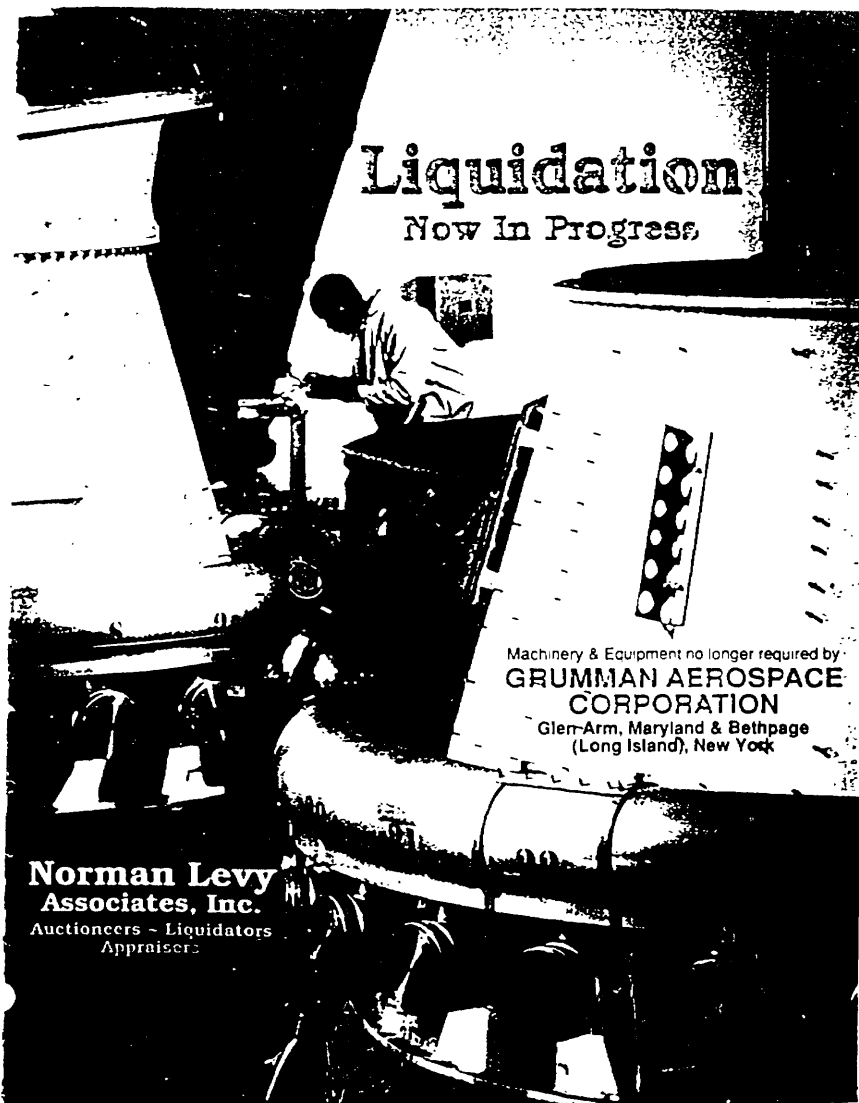
Lockheed Martin
Aeronautics Division
Littleton, Colorado

NORMAN LEVY
ASSOCIATES, INC.

Auctioneers / Liquidators / Appraisers

Headquarters: Southfield, Michigan

Offices in: Boston, Massachusetts • Chicago, Illinois
San Francisco, California • Coventry, England

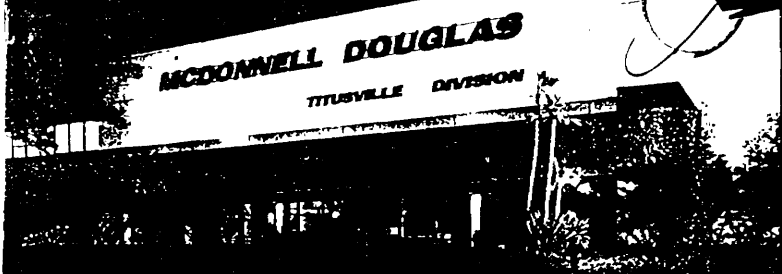


Liquidation
Now In Progress

Machinery & Equipment no longer required by
GRUMMAN AEROSPACE CORPORATION
Glen Arm, Maryland & Bethpage
(Long Island), New York

Norman Levy Associates, Inc.
Auctioneers - Liquidators
Appraisers

LIQUIDATION NOW IN PROGRESS



Surplus Machinery & Equipment no longer required in the continuing operations of

**MCDONNELL DOUGLAS
AEROSPACE EAST
FLORIDA MISSILE PRODUCTION
701 Columbia Blvd. • Titusville, Florida**

**Late Model CNC Machining Equipment
Testing Equipment**

Water Treatment System • Storage & Retrieval System • Chemical Process Lines

NORMAN LEVY ASSOCIATES, INC.

Headquarters: Phone 810-353-8640 • Fax 810-353-1442
21415 Civic Center Drive • Southfield, Michigan 48076

Boston, Massachusetts • Chicago, Illinois • San Francisco, California • Coventry, England

Auctioneers / Liquidators / Appraisers

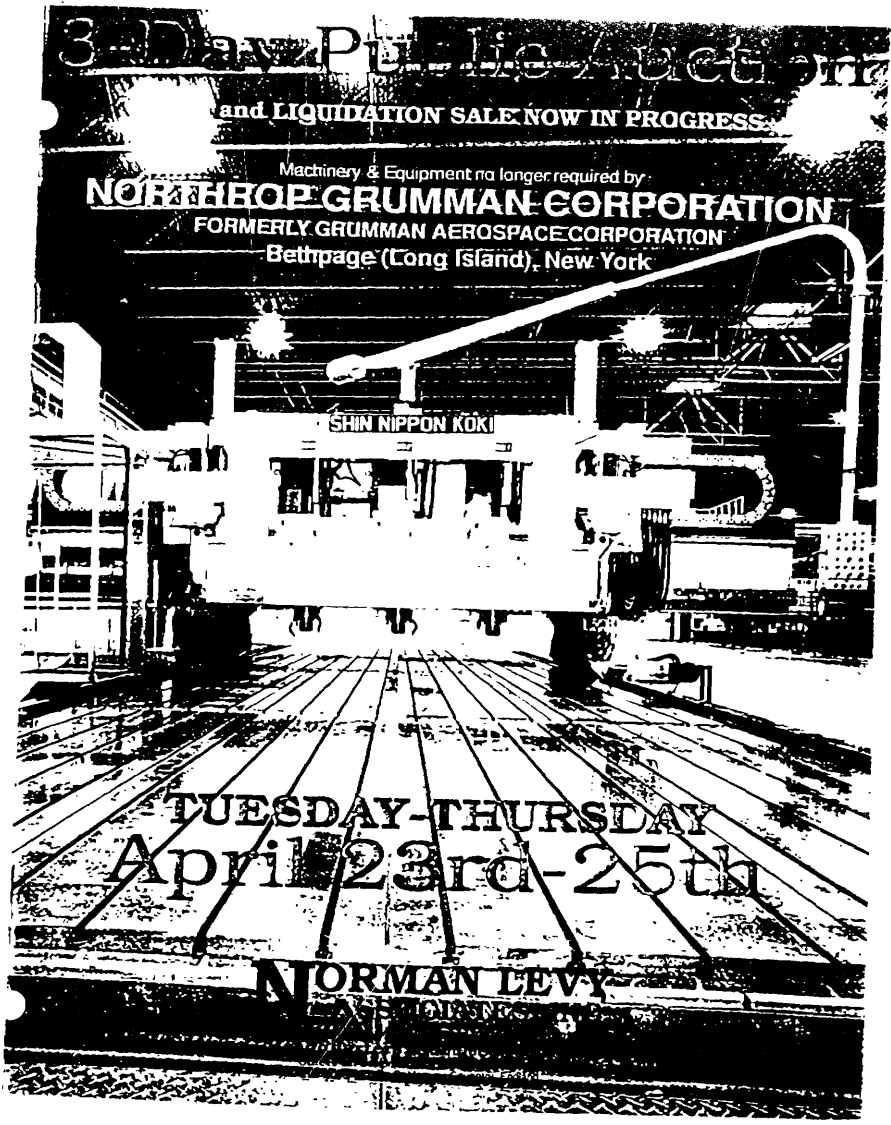
PUBLIC AUCTION

Surplus Machinery & Equipment no longer required in the continuing operations of
**MCDONNELL
DOUGLAS
AEROSPACE**
St. Charles & St. Louis, Missouri

**3-DAYS,
TUESDAY,
APRIL 30th
THROUGH
THURSDAY,
MAY 2nd**
BEGINNING 10 AM
(LOCAL TIME)
EACH DAY



ORMAN
SOCIETY
HERSHEY, PA. 17033
TEL: 717/533-1111
FAX: 717/533-1112



3-Day Public Auction
and LIQUIDATION SALE NOW IN PROGRESS

Machinery & Equipment no longer required by
NORTHROP GRUMMAN CORPORATION
FORMERLY GRUMMAN AEROSPACE CORPORATION
Bethpage (Long Island), New York

SHIN NIPPON KOKI

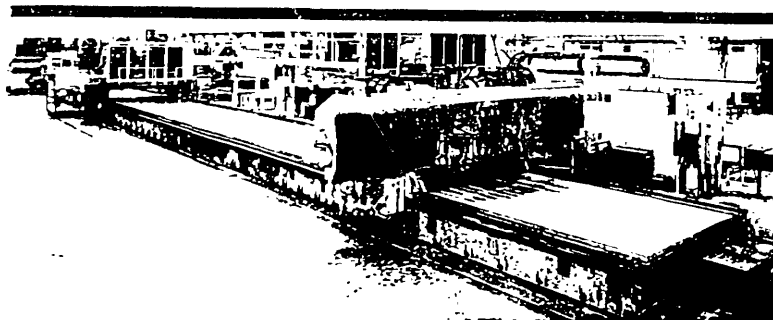
TUESDAY-THURSDAY
April 23rd-25th

NORMAN LEVY

2-Day Public Auction

and LIQUIDATION SALE NOW IN PROGRESS

Machinery & Equipment no longer required by
NORTHROP GRUMMAN CORPORATION
FORMERLY GRUMMAN AEROSPACE CORPORATION
12200 Long Green Pike • Glen Arm, Maryland



**TUESDAY &
WEDNESDAY**
**June 18th
& 19th**



**NORMAN LEVY
ASSOCIATES, INC.**

Auctioneers / Liquidators / Appraisers

Headquarters: Southfield, Michigan

Offices in: Boston, Massachusetts • Chicago, Illinois
San Francisco, California • Coventry, England

4-DAY PUBLIC AUCTION

& LIQUIDATION NOW IN PROGRESS

Machinery & Equipment
no longer required by

**GRUMMAN
AEROSPACE
CORPORATION**

*Manufacturing, Test
and Aircraft Support
Equipment*

TUESDAY-FRIDAY, AUGUST 15th-18th
Bethpage & Calverton (Long Island), New York

**NORMAN LEVY
ASSOCIATES, INC.**

Headquarters

21415 Civic Center Dr. • Southfield, Michigan 48076
Phone 810 353 8510 • Fax 810 353 1442

Boston, Massachusetts • Chicago, Illinois • San Francisco, California • Coventry, England
Auctioneers / Liquidators / Appraisers

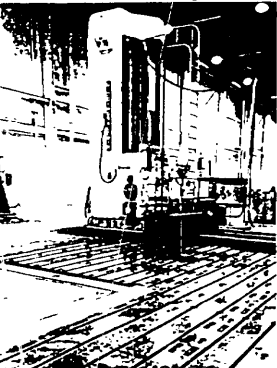
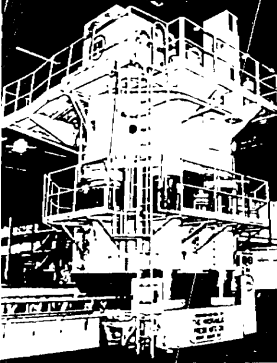
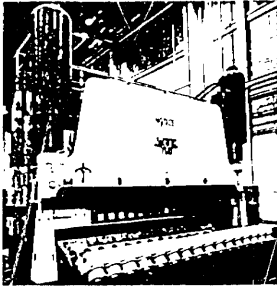
LIQUIDATION SALE NOW IN PROGRESS

Due to Complete Plant Closure,
Assets no longer required by

Lockheed
Abilene Facility
300 Wall Street
Abilene, Texas

**HERMAN LEVY
& ASSOCIATES, INC.**

Headquarters
21415 Olive Center Dr. • Southfield, Michigan 48076
Phone 810-353-8640 • Fax 810-353-1442
Boston, Massachusetts • Chicago, Illinois • San Francisco, California • Coventry, England
Auctioneers / Liquidators / Appraisers



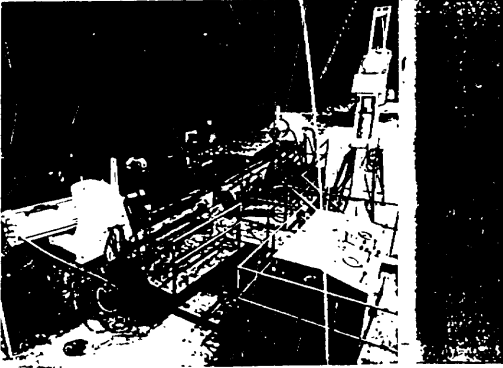
PUBLIC AUCTION

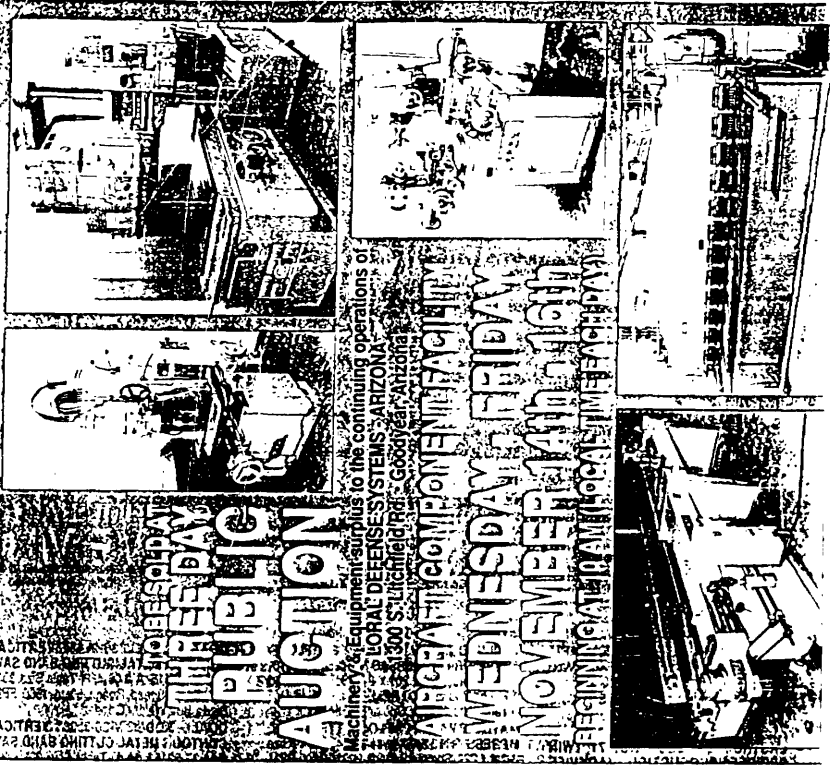
By Order of the City of Tulsa, Assets formerly belonging to
UNITED STATES AIR FORCE
 at Airforce Plant 30, Tulsa, Oklahoma

TUESDAY
SEPTEMBER 10, 1961

NORMAN DEAY
ASSOCIATES, INC.
Auctioneers / Brokers / Appraisers

Headquarters: Southfield, Michigan
 Offices: Boston, Massachusetts • Chicago, Illinois
 Dallas, Texas • Los Angeles, California • Coventry, England





WEDNESDAY - FRIDAY
 NOVEMBER 14th - 16th
PUBLIC AUCTION

Machinery & Equipment available to the continuing operations of
 LOCAL DEFENSE SYSTEMS - ARIZONA
 1900 S. Ritchfield Road - Goodyear, Arizona

AIR CRAFT COMPONENT FACILITY
 WEDNESDAY - FRIDAY
 NOVEMBER 14th - 16th
 BEGINNING AT 10 AM LOCAL TIME EACH DAY

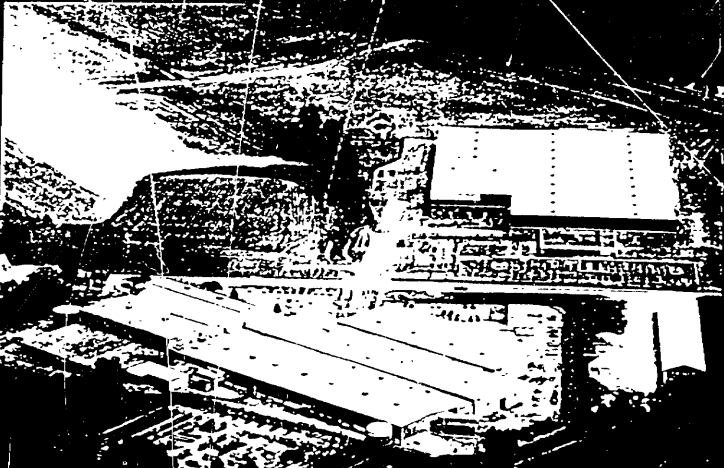
NORMAN LEVY ASSOCIATES, INC.
 Phone 313 253 8640 - Fax 313 253 1442
 21415 Civic Center Drive - Southfield, Michigan 48078
 Boston, Massachusetts - Coventry, England
 Auctioneers / Liquidators / Appraisers

First Class
 U.S. Postage
PAID
 Permit No. 1904
 Detroit, Mich.

WEDNESDAY - FRIDAY
 NOVEMBER 14th - 16th
 BEGINNING AT 10 AM LOCAL TIME EACH DAY

FIRST CLASS MAIL

ATTENTION PLANT MANAGER



365,000 Square Feet of Building Area - 45 Acres - Baltimore County, Maryland, U.S.A.

**COLLIERS
PINKARD**

Sheila Bennett, President
703-577-0001

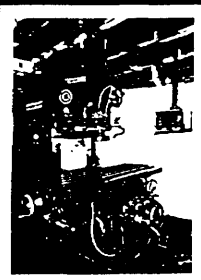
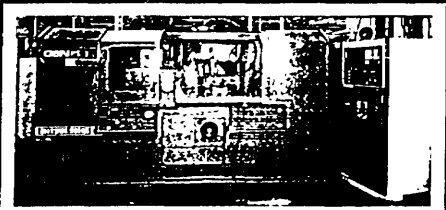
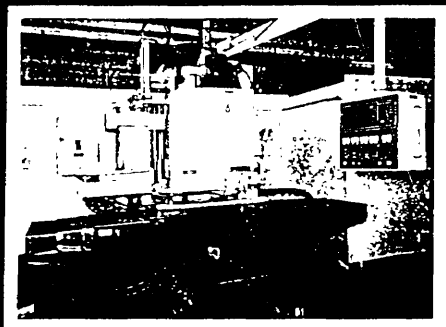
2-DAY PUBLIC AUCTION

Surplus Machinery & Equipment no longer required in the continuing operations of
MCDONNELL DOUGLAS
AEROSPACE



2600 North 3rd Street
 St. Charles, Missouri

**TUESDAY &
 WEDNESDAY**
JUNE 3rd & 4th
 Beginning at 10 am Each Day

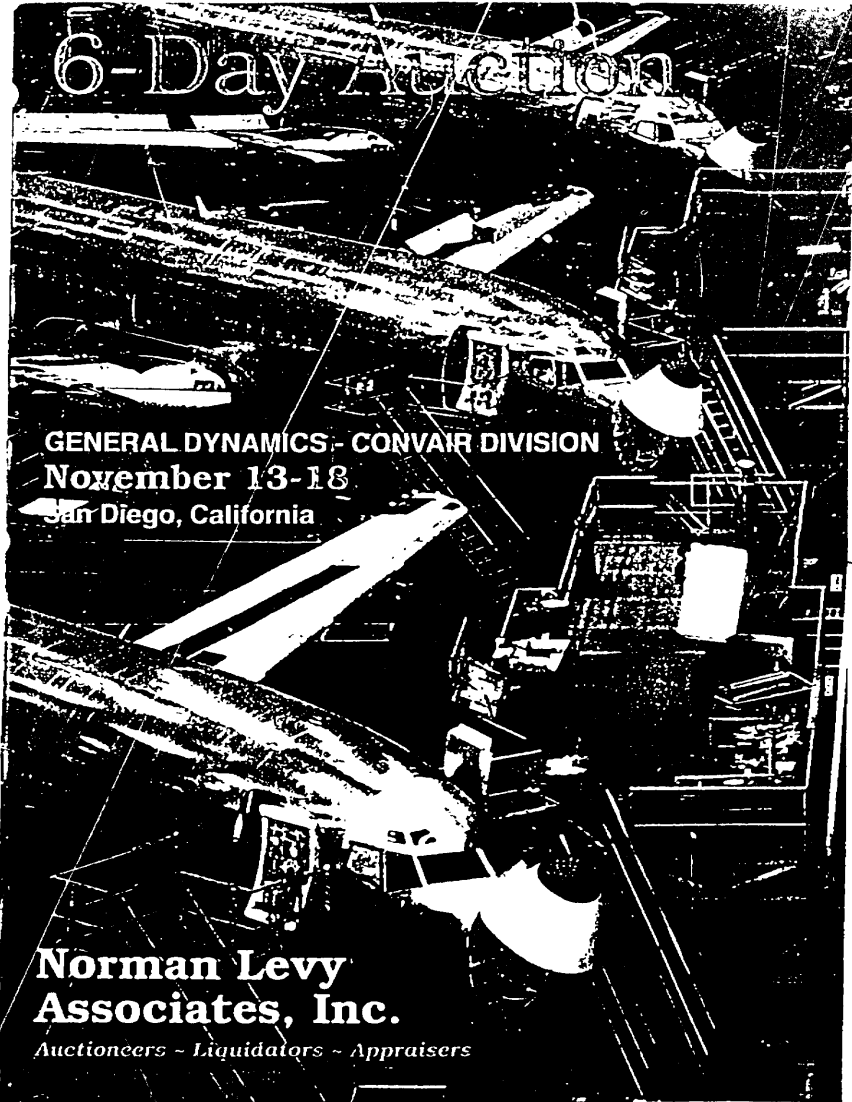


CNC Machining Centers
CNC Turning Center
CNC Thread Grinder
CNC Chucking Center
CNC Mills

Toolroom Machines

**Assembly, Inspection, Lab, Heat Treat,
 Electronic Test Equipment, Finishing,
 Aircraft Support, Material Handling,
 Food Service, Reproduction,
 Computer & Office Equipment**

NORMAN
ASSOCIATES
 Auctioneers

An aerial, high-contrast black and white photograph of a large industrial facility, likely an aircraft manufacturing plant. The image shows complex structures, including what appears to be a large hangar or assembly area with a curved roof. The text is overlaid on the image in a stylized, high-contrast font.

6-Day Auction

GENERAL DYNAMICS - CONVAIR DIVISION
November 13-18
San Diego, California

Norman Levy
Associates, Inc.
Auctioneers - Liquidators - Appraisers

PUBLIC AUCTION

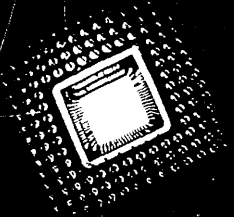
Due to Plant Closure, machinery & equipment of



ALCOA

ALCOA ELECTRONIC PACKAGING, INC.
San Diego, California

WEDNESDAY, SEPTEMBER 25th



NORMAN LEVY
ASSOCIATES, INC.

Auctioneers - Liquidators - Appraisers

AUCTION

HIGHWAY TRACTORS
 TRAILERS
 HYDRAULIC CRANE
 15 FORKLIFT TRUCKS TO 1994
 TOW TRACTORS
 AMBULANCE
 CARS & PICK-UP TRUCK
 OVER 25 ELECTRIC CARTS
 OVER 1600 PNEUMATIC TOOLS
 AGING OVENS
 FREEZERS
 PACKAGING EQUIPMENT
 WOODWORKING EQUIPMENT
 GANTRY ROUTER
 TOOLROOM EQUIPMENT
 X-RAY SYSTEMS
 FILM PROCESSING EQUIPMENT
 OPTICAL EQUIPMENT
 INSPECTION & TEST EQUIPMENT
 ASSORTED RACKING
 SHOP & FACTORY EQUIPMENT
 CLOSED CIRCUIT CAMERA SYSTEM
 OFFICE EQUIPMENT

Machinery & Equipment
 no longer required by

**GENERAL
 DYNAMICS**
 CONVAIR DIVISION
 3302 Pacific Highway, Gate 11
 San Diego
 California

WEDNESDAY & THURSDAY
FEBRUARY
14th & 15th
 BEGINNING AT 10 AM EACH DAY

Na **NORMAN LEVY ASSOCIATES, INC.**
 Headquarters: Phone 810-353-8640 • Fax 810-353-1442
 21415 Civic Center Drive • Southfield, Michigan 48076
 Boston, Massachusetts • Chicago, Illinois • San Francisco, California • Coventry, England
Auctioneers / Liquidators / Appraisers

ATTACHMENT C

Dual-Use Initiative: Facilitating Increased Costs and Rising Threats

Mil Spec Issues

Decontrol of dual-use technology

US MIL & Enemy will be swimming in same gene pool of tech

US procurement cycle will throw us behind hostile capabilities

Installed base, upgrade cost & frequency

The enormous size, diversity, and sunk cost in military spare parts makes it virtually impossible to keep pace with commercial technological capabilities for fielded systems. Downstream issues of interoperability, interchangeability and compability internally, and w/allies, generates additional costs & delays.

The length of time required to field new generations of U.S. weapons systems vs. the time and cost required for hostiles to acquire new threat capabilities is disproportionate. Generational leapfrogging = higher incentives and greater payback for overseas weapons builders than for U.S. incremental upgrades

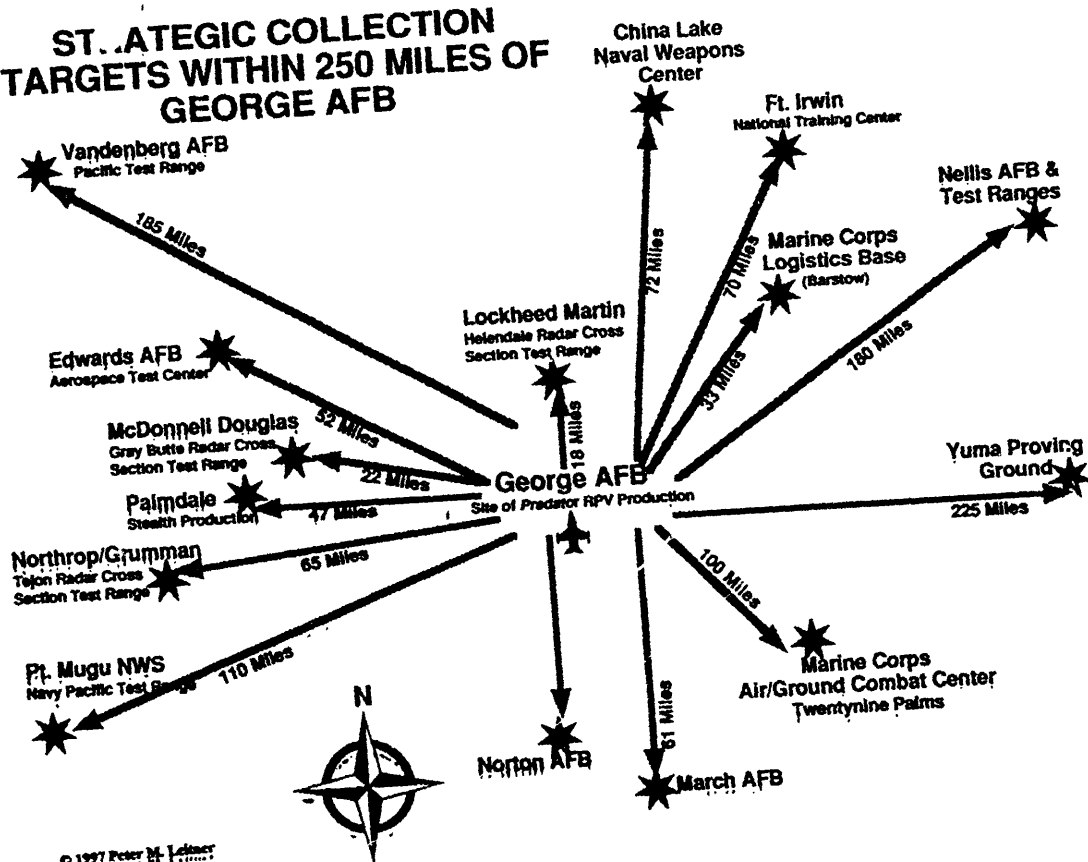
Potential hostiles will be given access to the identical commercial technology stock that the U.S. military will be forced to draw upon. Threats will be compounded by Joint Ventures, licensed production and other hands-on skills transfer mechanisms which will boot-strap overseas designers, manufacturers, and integrators with state-of-the-art techniques and QA.

Raising the stakes abroad. Access to advanced US manufacturing resources, skills and state of the art techniques will hemorrhage. This will be most apparent in aerospace & other power projection areas. Advanced conventional weapons threats must be ignored or undersold lest it undermine the goal of an export-led economic policy.

Shake-out in the U.S. defense sector will result in fewer system integrators and a return to turn-of-the-century industrial trusts. Second sourcing, creativity, reliability, and cost issues will come to the fore. Nation cannot afford to treat most large procurement contracts like non-competitive "black programs."

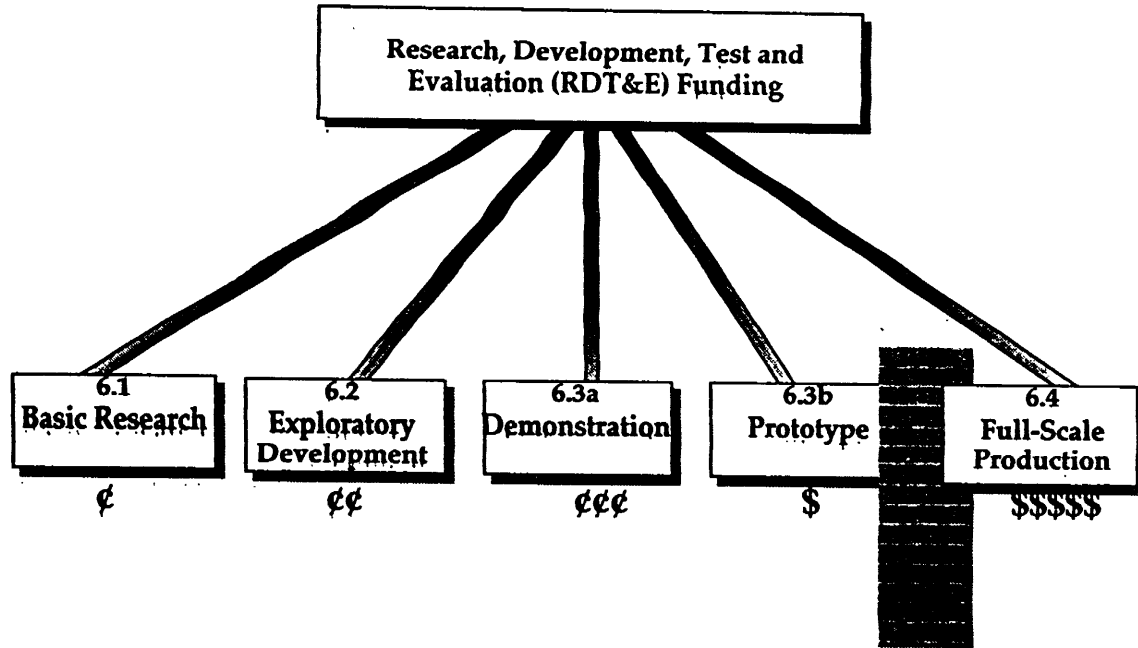
ATTACHMENT D

STRATEGIC COLLECTION TARGETS WITHIN 250 MILES OF GEORGE AFB



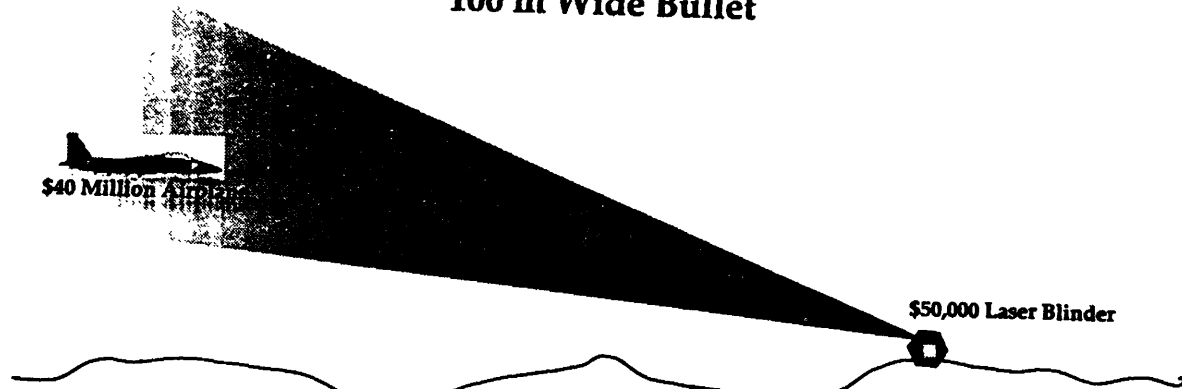
ATTACHMENT E

New PRC Threat to Break-Down Spending Firewall Between Prototyping and Full Funding of Industrial Base



ATTACHMENT F

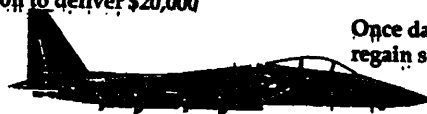
At 10,000 Meters Equivalent to Firing a 100 m Wide Bullet



- Easy Sell to public
- Very large pay-off for industrial base
- Use against civil aviation
- Use as assassination or terrorist weapon
- Humanitarian issue in U.N.
- Tactical weapon requires non-linear response
- More usable than Chem., Bio., or Nuclear weapons
- \$40 Million plane w/\$20 million laser protection
against a \$50,000 weapon to deliver \$20,000
worth of explosives

20 mrad Beam Divergence	
1,000 m	= 13 m Blinding Zone
2,500 m	= 33 m Blinding Zone
5,000 m	= 52 m Blinding Zone
10,000 m	= 104 m Blinding Zone

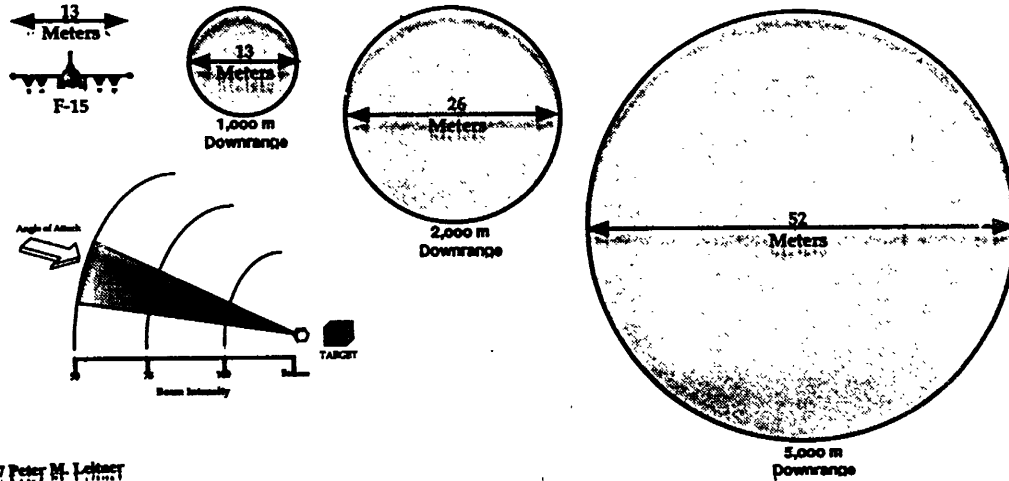
Once dazzled, a pilot has less than 28 seconds to
regain sight before ejecting or losing control



Tactical Use of Laser Blinding Weapons

Range (Meters)	Relative Beam Intensity	Volume of Airspace Effected	Lethality Within Envelope	Mission Consequences
5,000	100 %	3,536,109 m ³	Hemorrhage. Permanent Blindness	Loss of Aircraft and Crew
10,000	75 %	28,288,872 m ³	Retinal Damage, Cataracts Form, Permanent Damage	Loss of Aircraft and Crew
15,000	50 %	95,474,943 m ³	Dazzling, One Second to Two Minutes Recovery Time	Reduced Effectiveness to Total Loss Depending Upon Pilot Reaction

DOWNRANGE ILLUMINATION FIELD



Synergistic Effect of Decontrolling Laser Technology

Solutions	Costs	Effectiveness
Sealed Cockpit: No windows or protective shell around pilot when entering high threat environment.	Tens of \$ Billions	Most Effective. Technology does not yet exist. Current sensors are as vulnerable as human eye to laser exposure.
Brilliant stand-off weapons: Autonomous fire and forget, high precision, munitions carriers using multi spectral sensor arrays.	\$ Billions	Poor Tactical Substitute. Extreme cost, small warheads, on-board sensors vulnerable.
Volumeetric on-board defense system: Mini-lasers on aircraft project diffuse Laser pattern to polarize or ionize flight envelope as barrier to hostile Lasers.	\$ Billions	Doubtful utility. Technology does not yet exist. Special sensors needed to "see through" defense barrier, active barrier will increase electro-optical detectability of aircraft.
Countermeasures: Reflective, scattering, absorptive, material deployed between laser source and target.	Hundreds of \$ Millions	Doubtful utility against fixed targets, ineffective against mobile targets.
Anti-Laser homing missiles: Detect and ride beam back to source and destroy it.	Hundreds of \$ Millions	Minimally Effective, easy to counter.
Personal protective devices: Eyeglasses, shutters, visors, etc.	Tens of \$ Millions	Least effective, narrow bandwidth

ATTACHMENT G

FUTURE WEAPONS SYSTEMS: Microelectronic Technologies Required

- ★ ESSENTIAL
- IMPORTANT
- HELPFUL

	1985-1990	1990-1995	1995-2000	2000-2005	2005-2010	2010-2015	2015-2020	2020-2025	2025-2030	2030-2035	2035-2040	2040-2045	2045-2050	2050-2055	2055-2060	2060-2065	2065-2070	2070-2075	2075-2080	2080-2085	2085-2090	2090-2095	2095-2100	
Automated Production	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
CAD Equipment	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Chemical Plasma Etchers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Clean Room Design and Filters	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Cryochilled Crystal Pullers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
E-Beam Mask Makers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Epitaxial Growth (VPE, MBE)	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
High-Power Packaging Know-How	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
High-Purity Polyimides	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
High-Speed Gate Know-How	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Ion Implanters	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Ion Millers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Know-How to Optimize for Military	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Low-Pressure CVD	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Magnetically-Enhanced Sputtering	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Materials Characterization	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Optimized Layout Know-How	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Parametric Testers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Reactive Ion Etchers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Sensing & Stopping Proj. Aligners	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
VLSI Circuit Testers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Water Probe Testers	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Wire Bonders	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
100% Pin Packaging Know-How	★	●	★	★	●	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★

FUTURE WEAPONS SYSTEMS: Microelectronic Technologies Required

- ★ ESSENTIAL
- IMPORTANT
- HELPFUL

	Automated Production	CAD Equipment	Chemical Plasma Etchers	Clean Room Design and Filters	Carbide/Crystal Pullers	E-Beam Mask Makers	Epitaxial Growth (VPE, MBE)	High-Power Packaging Know-How	High-Purity Polysilicon	High-Speed Gate Know-How	Ion Implanters	Ion Millers	Know-How to Optimize for Military	Low-Pressure CVD	Magnetically-Enhanced Sputtering	Materials Characterization	Optimized Layout Know-How	Parametric Testers	Reactive Ion Etchers	Scanning & Stepping Prod. Aligners	VLSI Circuit Testers	Wafer Probe Testers	Wire Bonders	100+ Pin Packaging Know-How
Automated Production	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
CAD Equipment	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Chemical Plasma Etchers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Clean Room Design and Filters	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Carbide/Crystal Pullers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
E-Beam Mask Makers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Epitaxial Growth (VPE, MBE)	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
High-Power Packaging Know-How	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
High-Purity Polysilicon	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
High-Speed Gate Know-How	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Ion Implanters	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Ion Millers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Know-How to Optimize for Military																								
Low-Pressure CVD	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Magnetically-Enhanced Sputtering	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Materials Characterization	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Optimized Layout Know-How	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Parametric Testers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Reactive Ion Etchers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Scanning & Stepping Prod. Aligners	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
VLSI Circuit Testers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Wafer Probe Testers	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
Wire Bonders	★	★	★	★	●	★	●	●	★	★	●	○	★	★	●	★	★	★	★	★	★	★	★	★
100+ Pin Packaging Know-How	★			●																				★

ATTACHMENT H

IMPACT OF HOT SECTION DECONTROL

Decontrol by metaphor will yield the greatest results. Terms such as "Hot section" have no intrinsic meaning and can be defined to fit a particular audience. In addition, use of the term carries a certain rhetorical appeal as it can be argued that limited risks are being taken because it is only for one small part of an engine and will be limited to civil engines. This will effectively mask the equal utility of the underlying technology in military engines. Technologies, Materials, and components which will become free from export restraints by decontrol of "civil" hot sections include:

Materials:

- Superalloys
- Ceramic Matrix Composites
- Metal Matrix Composites
- Organic Matrix Composites
- High Temperature Bearing Steels
- Intermetallics
- Powder Metallurgy
- Fluorinated Polyimides
- High Modulus Organic Fibers
- Elastomers, Monoplasts, Phenolic Resins
- Carbon/Carbon Matrix
- Silicon Carbide Matrices

Coatings:

- Aluminides
- Platinum-Aluminides
- Silicides
- Carbides
- Refractory Metals

Coating Systems:

- Chemical Vapor Deposition (CVD)
- Physical Vapor Deposition (PVD)
- Thermal-Evaporation PVD (TE-PVD)
- Electron-Beam PVD (EB-PVD)
- PVD-Resistive Heating
- PVD-Cathodic Arc Discharge
- Pack-Cementation
- Plasma Spraying
- Slurry Deposition
- Sputter Deposition
- Ion Implantation
- Ion Plating
- Laser Hardening

Bearings:

- Solid Ball and Roller
- Gas-Lubricated Foil Bearings
- Hydrostatic Fluid Film Bearings
- Active Magnetic Bearings
- Shaverth & Adore CAD Programs

Software:

- Gas Turbine CGD s/w
- 2D or 3D Viscous s/w for Engine
- Flow Modeling

Technology:

- Thin Wall Cooling
- Hot Isostatic Presses
- Machine Tools
- Electro-discharge Machines
- Ceramic Core Manu. Equip.
- Ceramic Shell Wax Pattern Prep. Equip.
- Gas Turbine Brush Seal Manu. Equip.
- Tools, Dies, & Fixtures for Solid State Joining
- Precision Hole Drilling
- Single Crystal. Directionally Solidified Blade Manu. Equipment
- Precision Investment Casting
- Water Jet Machining
- Forging
- Diffusion Bonding
- Cooled & uncooled turbine blades
- Airfoil to disk techniques

Components:

- Heat Exchangers
- Single Crystal. Directionally Solidified Blades
- Ceramic Cores & Shells for Airfoils & Vanes
- Thermally Decoupled Combustion Liners
- Multi-domed Combustors
- Non-Metallic Liners

ATTACHMENT I

Dr. Peter M. Leitner

Publications

Books:

- Decontrolling Strategic Technology, 1990-1992: Creating the Military Threats of the 21st Century. (Lanham, Md: University Press of America, 1995).
- Reforming the Law of the Sea Treaty: Opportunities Missed, Precedents Set, and U.S. Sovereignty Threatened. (Lanham, Md: University Press of America, 1996).
- NANSHA: War in the South China Sea. (Forthcoming, Winter 1998) [Fiction]
- Handbook of Quality Management. (New York, N.Y.: Marcel Dekker Publishers, Inc., Fall 1998)
Co-edited volume under contract with publisher.
- Waging Guerrilla Warfare Within Large Organizations: A Tactical Survival Guide. (In progress.
Projected publication, Winter 1999)

Articles:

- "Ethics, National Security and Bureaucratic Realities: North, Knight, and Designated Liars," American Review of Public Administration, Vol. 27 No. 1, March 1997: 61-75. Coauthored with Ronald Stupak.
- "Japan's Post-war Economic Success: Deming, Quality, and Contextual Realities," Journal of Management History. (Forthcoming Summer 1997).
- "Eyewitness to History: Methodological Suggestions, Public Servant Perspectives, and Professional Publications," (Forthcoming Fall 1997).
- "Supercomputers, Test Ban Treaties, and the Virtual Bomb," (Forthcoming Fall 1997).
- "A Bad Treaty Returns: The Case Against the Law of the Sea Treaty" (Forthcoming Fall 1997)

Government Technical Reports:

- STEM. Refractory Materials. (Paris, 1991). *
- STEM. Production Equipment for Non-Electronics. (Paris, 1991). ***
- STEM. Non-Linear Optical Materials. (Paris, 1991). *
- STEM. Structural Ceramics. (Paris, 1990). *
- STEM. Carbon-Carbon Composites. (Paris, 1990). **
- STEM. Shape Memory Alloys. (Paris, 1990). *
- STEM. Nickel & Cobalt Superalloys. (Paris, 1990). *
- STEM. Production and Test Equipment for Electronics. ***
- STEM. Superconductive Ceramic Oxides. (Paris, 1989). **
- STEM. Powder Metallurgy. (Paris, 1989). *
- STEM. Radar Absorbent Materials/Structures. (Paris, 1988). **
- STEM. Aluminum-Lithium. (Paris, 1988). *
- STEM. Aluminides. (Paris, 1988). *
- STEM. Organic Matrix Composites. (Paris, 1987). *
- STEM. Metal Matrix Composites. (Paris, 1987). *

Government Policy Reports:

- U.S. General Accounting Office. Uncertainties Surround the Future of U.S. Ocean Mining. NSIAD-83-41 (September 6, 1983).**
- U.S. General Accounting Office. U.S. Role in Sinai Important to Mid-East Peace. ID-82-62 (September 9, 1981).**
- U.S. General Accounting Office. Forging a New Defense Relationship With Egypt. ID-82-15 (February 5, 1982).*
- U.S. General Accounting Office. U.S. Overpays for Suez Canal Transits. (ID-82-19 (February 10, 1982).**
- U.S. General Accounting Office. Military Damage Claims in Germany -- A Growing Burden. ID-81-4 (October 9, 1980).*
- U.S. General Accounting Office. Status of Accounting Education in the Third World. ID-80-25 (January 1980).****
- U.S. General Accounting Office. Law of the Sea Conference -- Status of the Issues, 1978. ID-79-6 (March 9, 1979).**

Government White Papers:

- Department of Defense. *U.S. / India Relationship: What are the Groundrules?* (December 1990).
- Department of Defense. *Garrett Engines to the PRC: Enabling Their Long-range Cruise Missile Program*. (May 1991).
- Department of Defense. *McDonnell Douglas Machine Tool Sales to the PRC: Implications for U.S. Policy*. (June 1994).
- Department of Defense. *Transferring Stealth Technology to the PRC: Three Pieces to the Chinese Puzzle*. (December 1994). Co-authored w/Peter Gauthier.
- Department of Defense. *Nuclear Safety, Strategic Technologies, and Weapons Proliferation: A New Approach*. (October 1995).
- Department of Defense. *Non-Nuclear, Militarily Critical Uses of Oscilloscopes* (December 1996).

- * Chairman of Study Group and Contributor.
- ** Chairman of Study Group and Principal Author.
- *** Head of U.S. Delegation and Contributor.
- **** Team Member: Co-author of Philippines Section.

RADIO FREQUENCY WEAPONS AND THE INFRASTRUCTURE

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

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.

2 sided copy

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.

CHINA AND ECONOMIC ESPIONAGE

by John Fialka

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

Isidore G. G. G.

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 ensnared 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."

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."

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 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.

###

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

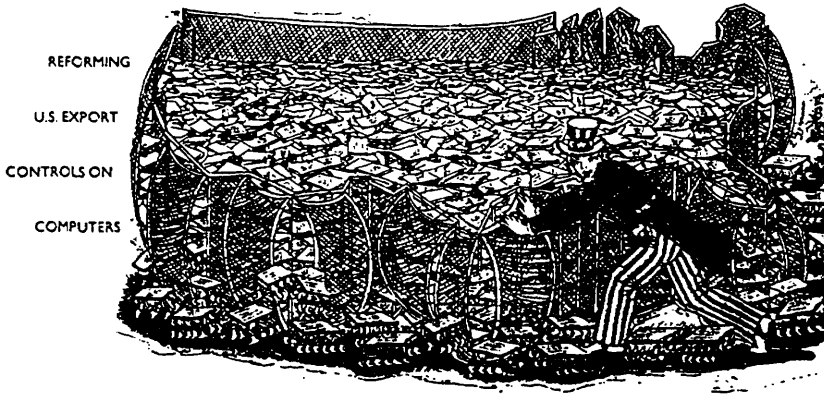
- of 10, China scored 2.16, ranking it just above Indonesia, which was in last place.
11. Woolard made his remark in November 1995 at a symposium on international security issues at the State Department.
12. "Civil-Military Integration; The Chinese and Japanese Arms Industries," a background paper published 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.

2-sided copy

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

24. Interview with Finn, Sept. 1995.

CONTROLLING THE



KENNETH
FLANN

Last October the Clinton administration unveiled its second major reform of U.S. export control policies for powerful computers. The 1995 reforms, coming only two years on the heels of an earlier loosening of controls, further eased sales of high-powered U.S. computers abroad. Just prior to the announcement, Floyd Spence, chairman of the House National Security Committee, and Ron Dellums, the committee's top Democrat, had written to President Clinton objecting to any relaxation of supercomputer controls. Though the reforms were supported by the *Washington Post* and the *New York Times*, critics of varied political stripes, from nonproliferation activist Gary Millhollin to defense hawk Frank Gaffney, lashed out at the new policy.

No one involved in the ongoing policy reform effort—and I know, because I was part of it—had any intention of handing America's military adversaries greater access to more powerful computers. What drove both the 1993 and the 1995 decisions to loosen controls on computer exports was the recognition that the ongoing revolution in information technology had left the export control system behind.

High-performance computers are now ubiquitous in everyday life. They are as likely to be used to design a high-tech toaster or provide special effects for Disney's latest film as to help produce advanced armaments. And more and more, everyday personal computers are pushing against yesterday's "supercomputer" threshold.

I recently bought a \$2,400 personal computer from an unsophisticated local clone PC dealer. He sells systems made from Chinese cases and power supplies, Taiwanese circuit boards, Taiwanese and Korean memory and logic chips, Korean monitors, and disk drives manufactured in Singapore, Taiwan, and Thailand. The only part in these systems that must be supplied by U.S. manufacturers is their Pentium processor chip, sold in the tens of millions around the globe. Under the control regime in place before the 1993 reforms, anyone planning to market my PC abroad would have worried about a costly process of filing for special licenses and prior approval from the U.S. government. In 1992, about half of these cases raised no questions, with a licensing decision reached in an average of 9 days; the balance averaged 50 days.

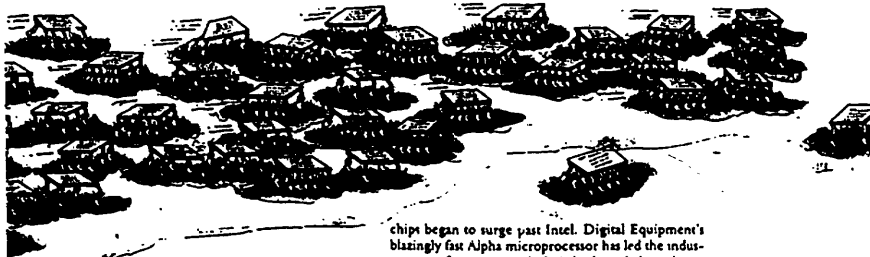
If my PC had been equipped with a more expensive (but widely available) dual Pentium circuit board (made in Taiwan), it would have been classified as a "supercomputer" and given a prospective exporter *real* headaches. Supercomputers may require continued monitoring of computer use after a sale, with usage logs, audits, and other safeguards against unauthorized use, as well as prior approval.

Restricting the export of PCs that a gifted junior high school graduate in India or Singapore can easily put together from off-the-shelf parts does nothing for U.S. national security. The key Defense Department interest in today's computer market is not to try to control the uncontrollable, but to guarantee itself an industrial base that can provide it with the most ad-

THE BROOKINGS REVIEW

VOLUME 11 NUMBER 4 WINTER 1995

UNCONTROLLABLE



vanced information technology in the world, before it is available to others. Yesterday's export control policies actually handicapped our industrial base in an increasingly competitive foreign market (more than half U.S. company sales). More important, by creating significant foreign markets not easily accessed by U.S. firms, controls provided overseas competitors protected niches from which to challenge the dominance of the U.S. computer industry—and the technological advantage at the very heart of U.S. military strategy.

Silicon Realities

The U.S. export control system has traditionally had twin objectives: where feasible, to deny (or more realistically, render difficult and costly) a potential adversary's access to critical military capabilities and to track the ultimate destinations for goods with particularly significant military potential. The administration's new approach to controlling exports of computers maintains those two objectives while responding to technological reality.

Figure 1 plots performance ratings for the products of several major U.S. microprocessor chip companies over the past decade, along with new offerings slated to be shipped through 1997. The tale it tells is extraordinary.

Since 1991 the U.S. government has measured the performance of the silicon microprocessor chips that drive modern electronic systems with an arcane metric known as MTOPS: millions of theoretical operations per second. For the past 10 years, industry leader Intel's microprocessor chips' performance has been improving tenfold every five years, a trend that shows no sign of slowing (see figure). In the early 1990s, a new, non-Intel RISC (reduced instruction set computer) microprocessor chip technology was introduced, and by the mid-1990s some of these hot new

chips began to surge past Intel. Digital Equipment's blazingly fast Alpha microprocessor has led the industry in performance, with their high-end chips almost a full order of magnitude faster than Intel's mainstream product. And chips from companies like Sun and MIPS have joined DEC in the lofty heights above the Intel trend line.

In 1993 the computer export control line was drawn at 12.5 MTOPS, the supercomputer line at 195 MTOPS. But by then shipments of Pentium-based PCs performing at 60 MTOPS or greater were already taking off, and sales of the microprocessor on which they were based were effectively impossible to control (how can one track tens of millions of units the size of a postage stamp?). In addition, with so-called PC chip sets (several logic chips containing all of the circuitry needed for a PC) widely available right off the shelf, a relatively unsophisticated technician could easily put together a personal computer exceeding the decontrol limit. Indeed, Taiwanese companies using such chip sets (many of which were also manufactured in Taiwan) soon were producing most of the PC circuit boards into which Intel's computer chips were being plugged.

In effect, the pre-1993 U.S. export controls made it tougher for American computer companies to compete against Asian firms producing systems using what were fundamentally the same American high-tech components. Taiwanese firms, for example, were able to freely sell late-model PCs they manufactured in markets where U.S. vendors of equivalent models had to apply for export licenses.

And a new technology trend threatened to make the situation even worse. With the introduction of the Intel Pentium chip, a new mass market computing technology, the so-called symmetric multiprocessor (SMP) system, was maturing. In 1993 several chip manufacturers announced that SMP chip sets, which made it relatively easy to put up to four Pentium chips on a single circuit board, would soon be commercially available. SMP computers would be particularly attractive and cost-effective in providing data served to

Kenneth Flamm is a senior fellow in the Brookings Foreign Policy Studies program. From 1993 to 1995 he was principal deputy assistant secretary of defense (economic security) and special assistant to the deputy secretary of defense (dual use technology policy). He is coauthoring "Mismanaged Trade? Strategic Policy in the Semiconductor Industry."

other machines hooked to the networks of PCs invading the world's offices and factories. Off-the-shelf software, such as UNIX, Microsoft's Windows NT, IBM's OS/2, and Sun Microsystems' Solaris, would also be available to allow users to exploit the power of these "SMP boxes." While U.S. manufacturers were preparing to put together even more powerful servers and SMP workstations, using even more processors than these four-way systems, the forthcoming availability of these chip sets meant that the smaller-scale SMP boxes were going to be an instant battleground for international competition.

The 1993 Decontrol Decision: New Principles

With Intel poised to ship millions of even higher-performance Pentium processors over the next year and a half to two years, it was clear in 1993 that Asian companies would rapidly develop and sell Pentium SMP systems with up to four processors and ship products approaching 500 MTOPS performance by mid-1995. Roughly the same situation existed with the new RISC microprocessor chips coming to market in the non-Intel world.

Thus the first Clinton administration reforms decontrolled computer exports to 500 MTOPS and imposed after-sale monitoring on only the most powerful computing machines. With machines shipped in the millions, or even hundreds of thousands, there is no realistic hope of tracking access, but the market for the very highest-performance computing systems is relatively small. To protect a desired one to two order-of-magnitude advantage in supercomputers by the United States and its close allies, the administration proposed the strictest controls on exports of computers above 2,000 MTOPS (though it was able to negotiate only 1,500 MTOPS in bilateral discussions with Japan, the only other country making high-powered machines at the time). Finally, recognizing frankly that computer technology was a speeding train to which the government was barely hanging on, the administration agreed to re-examine these limits with a year and a half to two years.

In retrospect, the 1993 reforms were eminently sensible. Today many vendors around the globe sell four-processor SMP Pentium boxes, and even I can assemble a PC exceeding the 1993 supercomputer limit from imported, mail-order parts. International consortia and alliances abound in even higher-performance microprocessor technologies. The increasing globalization of computer technology is a striking new fact of industry life.

In reshaping the 1993 policy, the administration had also developed three clear principles that would prove useful again in revisiting high-tech export controls. First, accept the impossibility of controlling the uncontrollable. Avoid shooting our own defense industrial base in the foot to no useful effect. Second, make a sensible prospective policy. Because making major changes in export controls takes the better part of a year, or more, a new policy should be designed to stick for at least a couple of years. In rapidly moving high-tech areas, fixing tomorrow's control levels at today's international availability virtually guarantees creating at least a temporary competitive edge for foreign challengers to

the U.S. industrial base. And third, limit controls to what is of real military significance. Controls make sense only if they prevent an adversary from doing something significant that cannot be done with widely available systems.

Revisiting Reality in 1995

A relentless technology revolution made reform even more complex in 1995. The mid-1990s jump in microprocessor power was inducing an analogous jump in the power of workstations using those chips. Even more important, the first ripples from the early SMP workstations were swelling into a virtual multiprocessor tidal wave sweeping the computer industry.

After years of research, so-called "scalable," parallel computer systems were taking off. Powerful new software tools were making it easier for users to divide complex problems into pieces that could be run separately on multiple processors, with the results then combined. The same programming model—and tools—could be used to break a problem up into pieces run within the tightly linked processors inside a massively parallel supercomputer, or the smaller number of processors within an SMP server, or even on individual workstations linked together over a local area network.

A three-pronged technological assault on the computing frontier was clearly under way. First, virtually all the powerful new U.S. microprocessors scheduled to ship through 1997 were designed to computer makers could easily lash together four processors in an SMP configuration on a single circuit card. Second, by connecting industry-standard interfaces with high-speed communication links, becoming widely available commodities on the open market, foreign computer makers—even the less sophisticated ones—were going to be able to connect multiple processor SMP boards together into very powerful systems. Third, a new generation of SMP operating systems (like Windows NT) would make it easy to use all this processing power simultaneously on multiple problems, while new parallel software tools would make it possible to harness this computing power on a single problem. Whether using multiple processors within a single SMP box or massive numbers of processors within a parallel supercomputer or many workstation and personal computers linked over a local area network, the world of high-performance computing was clearly going scalable.

Indeed, the U.S. supercomputer industry has bet its future on this trend. Essentially all major U.S. vendors of high-performance computing hardware have now clearly opted to pursue a "commodity microprocessor" strategy. They are gambling that by taking advantage of the low costs and rapid improvement in mass-market microprocessors, and focusing on better parallelization tools and higher-performance methods of interconnecting and coordinating these processors, they will be able to deliver more and cheaper massive computing power than their global competitors. They are taking a certain risk because their main Japanese competitors have focused their energy on using specialized chips to develop even faster versions of more traditional supercomputers that can run existing software. Because the new, scalable



microprocessor systems are generally less efficient (though considerably cheaper) in delivering usable computing power from aggregate system MTOPS, and often require software modification, an export control system that does not penalize use of the new machines is important to the survival of a U.S. high-performance computer industrial base.

These developments also mean that the supercomputer business will no longer be a bilateral U.S.-Japanese club. Already, European vendors are producing supercomputer-class machines from the same American components that U.S. vendors are using. Taiwanese and Korean producers will eventually follow suit.

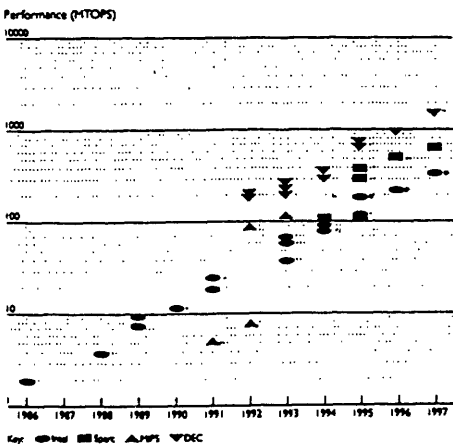
In developing its 1995 reform proposal, the Defense Department undertook to answer two key questions. The first was how much computing power would be widely available in desktop workstations on world markets over the next few years. Two independent studies and numerous inquiries pursued directly with U.S. industry concluded that U.S. vendors would introduce powerful new SMP workstations with performance up to 15,000 MTOPS over the next two years. Defining "widely available" products conservatively as those that had been on the market for two years, the Pentagon estimated that SMP workstations with performance of up to 7,000 MTOPS would be widely available by 1997.

The second question was what militarily critical applications should be controlled. With little gain evident from trying to control applications that could be parallelized and run on clusters of widely available workstations, this exercise turned into a hunt for the lowest performance level (not widely available) required by a nonparallelizable, militarily significant application. A consultant survey of defense applications came back with an answer: 10,000 MTOPS for quick turnaround, fine-grained tactical weather forecasting. Thus, 10,000 MTOPS emerged as the boundary for militarily significant capabilities that an export control regime might hope to deny to adversaries through 1997—by which time the government will again revisit the entire computer export control system from first principles, including an alternative to the outmoded MTOPS measure of performance that reflects today's new scalable computing paradigm.

The proposed new export control system announced last October decontrols computers below 20,000 MTOPS to America's closest allies, 10,000 MTOPS to most of the rest of the world, and 7,000 MTOPS for civilian uses in countries of nonproliferation concern. A virtual embargo continues on the "pariah" states, Iran, Iraq, Libya, and North Korea. These recommendations are the starting point for U.S. talks with member states of the "New Forum," the new multilateral export control regime set up in 1995 to take the place of CoCom, the old Cold War regime that expired in 1994.

These talks will not be easy. Although the United States has moved ahead in defining sensitive technology areas with its New Forum partners, no agreement has been reached on what information is to be shared among partners and on what terms. Without agreement on some regular and substantive information ex-

U.S. Microprocessor Performance Trends



change, it is hard to see how the control system can either restrict access to critical military capabilities or track the destination of goods with military potential.

At the moment, the only way the Pentagon can be sure it knows where high-performance computers are going is for U.S. companies (who are required to keep records of such exports and make them available to the government) to export them. Similarly, the best way for the Pentagon to be assured that the information technology it fields is the world's best is to have it supplied by a U.S. industrial base that dominates world technology and is willing to work closely with U.S. armed forces. Perhaps the key insight in the Clinton administration's export control policy reforms is the explicit recognition that the surest way both to preserve the critical U.S. technological edge in computers and to track the sales of high-performance computers worldwide is for America's computer industry to continue to blow away the foreign competition around the globe.

Critics will no doubt continue to berate the administration for raising the export bar. To follow their advice, however, would only fuel a dangerous and self-deceptive illusion of action. Maintaining the U.S. lead in this critical technology, in a world of intensifying international competition, is at the heart of this nation's future national security. ■

A Brief History of MTOPS

	1 Pentium Personal Computer	Easily Available SMP Pentium Workstation	High End Server/ Workstation	High End U.S. Commercial Supercomputer	Decontrol Level	Supercomputer Level
1993	66		1800	20000	12.5	195
1995	133	432 <i>(4 processors)</i>	7600	76000	500	2000
mid-1997	350/625 <i>(single/dual Pent II cartridge)</i>	1456 <i>(8 processors)</i>	32000	284000 <i>(>643000, R&D)</i>	2000-7000 <i>for most</i>	undefined

Kenneth Flamm
June 1997