1693

S. HRG. 105—570

TERRORISM AND INTELLIGENCE OPERATIONS

HEARING

before the

JOINT ECONOMIC COMMITTEE
CONGRESS OF THE UNITED STATES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

May 20, 1998

Printed for the use of the Joint Economic Committee

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1998

cc 50-229

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-057337-8

JOINT ECONOMIC COMMITTEE

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

Prepared for printing by DARRYL C. EVANS,
COLLEEN J. HEALY, AND
JUANITA Y. MORGAN

CONTENTS

OPENING STATEMENTS OF MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

TERRORISM AND INTELLIGENCE OPERATIONS

Wednesday, May 20, 1998

UNITED STATES CONGRESS,
JOINT ECONOMIC COMMITTEE,
WASHINGTON, D.C.

The Committee met, pursuant to notice, at 10:08 a.m., in Room 106, Dirksen Senate Office Building, the Honorable Jim Saxton, Chairman of the Committee, presiding.

Present: Representatives Saxton, McCrery and Sanford, and Senator Bennett.

Staff Present: Vaughn Forrest, Colleen Healy, Juanita Morgan, Joseph Cwiklinski, Dan Lara, and Darryl Evans.

OPENING STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

Representative Saxton. Good morning. I'm pleased to welcome our distinguished panelists before the Joint Economic Committee (JEC) this morning.

As we reach the end of this century and enter the next one, we must anticipate and prepare for the changes, new realities, and challenges that will come in the near future. How we handle those challenges will determine our success in the century ahead.

Unpreparedness and the exercise of bad judgment could put the United States in a significantly disadvantaged position economically and militarily, and could even threaten our national security.

It is the opinion of many experts, a few of whom will testify today, that terrorists and the intelligence services which support terrorists, will step up attacks using electro-magnetic pulse weapons and biological weapons. Terrorists will continue to deny responsibility while maintaining the capabilities to continue the high-profile attacks.

Many believe, as I do, that our success in high-technology warfare had deterred our enemies and, in many ways, contributed to the conclusion of the Cold War. Our continued success in the Gulf War made it very clear that the challenge ahead to the United States and that the conventional role that we played in the war was very successful.

It is this very success in conventional warfare that has caused those who disagree with the democratic process and the values of the West to create new weapons heretofore unknown.

While these new weapons are being developed, our enemies increasingly strengthen their commitment in terms of manpower, money, and intelligence service capabilities, particularly in the areas of covert actions, counter-intelligence, and surveillance.

That, I would suggest, could have significant impact on the national security and economic performance of the United States. We need to develop our capabilities against new and improved weapons of mass destruction and we will, hopefully, move to do so.

The Congress must be prepared to study Cold War institutions and examine the need to create new and dynamic organizations.

Before we begin, I would like to thank each of our witnesses for your very hard work, your dedication and commitment, which has oftentimes required great personal risk.

The United States is a better nation, and its citizens are much safer, because of your courage and dedication.

This morning, our first witness is Mr. Victor Sheymov, who defected to the United States from the Soviet Union in 1980. At that time, he was a major in the 8th Directorate of the KGB – the Russian equivalent of our National Security Agency. His last position in the KGB involved the coordination and responsibility for the overall security for the KGB foreign cipher communications.

Mr. Sheymov graduated from Moscow State Technological University, and was a researcher at the Russian Military Research Institute. He has also worked with the Soviet "Star Wars" program, and has written a book entitled, *Tower of Secrets*.

Our second witness, Dr. Kenneth Alibek, defected to the United States in 1992. At that time, Dr. Alibek was the First Deputy of the Soviet Union's Offensive Biological Warfare Program and a retired colonel of the Soviet Army. Dr. Alibek holds a medical degree in infectious diseases, a Ph.D. in microbiology, and a doctor of science in industrial biotechnology.

Dr. Alibek spent 21 years in pathogen laboratories studying the production of many types of biological weapons, such as plagues and anthrax. He also developed medical protocols for the treatment of these diseases and for the treatment of mass casualties caused by biological weapons.

Since his arrival in the United States, Dr. Alibek has worked with various government agencies and is currently continuing his work combatting biological weapons.

Our third witness is Dr. Nicholas Eftimiades, who currently works for the Defense Intelligence Agency. He is here today to discuss, at least in part, the context of his book, *Chinese Intelligence Operations*, which is considered to be the first ever scholarly analysis on the subject and has been translated into four languages.

He has also held positions in the CIA, with the counter-intelligence staff at the State Department, and has been a naval officer.

He has written numerous articles and a monograph entitled, "China's Ministry of State Security: Coming of Age in the International Arena." For this work, he was awarded the "Scholarly Work of the Year on Intelligence" by the National Intelligence Center. He is also the recipient of the Director's Intelligence Medal by the Defense Intelligence Agency.

Mr. Eftimiades graduated from George Washington University with a B.A. in East Asian studies and a Master's in strategic intelligence from the Joint Military Intelligence College.

As you may have noted, he is not here yet, but we are hoping that he will arrive in the next few minutes.

Our final witness is Mr. Brian Fairchild. From September 1976 to October 1995, Mr. Fairchild was a staff operations officer in the directorate of operations at the Central Intelligence Agency.

Mr. Fairchild is a former member of the Army's elite special force–the Green Beret. He is a graduate of California State University with degrees in international relations and Asian studies and speaks several Asian and European languages.

Mr. Fairchild is now retired from the CIA and owns his own company on the West coast.

Thank you all again for being here. We appreciate it very much.

And at this time, we'll begin with Mr. Sheymov. I understand your testimony will take something under 10 minutes. We will, incidentally, have to take a break sometime between 11:00 a.m. and 11:15 a.m., or thereabouts, as there will be a vote on the House side.

So Mr. Sheymov, if you would begin, we appreciate very much your being here.

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

OPENING STATEMENT OF VICTOR SHEYMOV, COMSHIELD CORPORATION

Mr. Sheymov. Mr. Chairman, first of all, I would like to thank you and the Members of the Committee for your attention to the problem of terrorism and to recent attempts of different parties to take advantage of the technological achievements of this country.

I also would like to thank you for inviting me with an offer to share my views on some of the high-tech problems, which I spent about 27 years of my life studying and specializing in.

Representative Saxton. Sir, may I just ask you to pull the microphone just a little bit closer?

Mr. Sheymov. Okay. Is that better?

Representative Saxton. Fine.

Mr. Sheymov. RF weapons, which were discussed in this Committee before, it's a pretty wide range of – Mr. Chairman, I would like to ask your permission to have my written statement entered into the record.

Representative Saxton. Certainly. In fact, all written statements will be included in the record.

Thank you.

Mr. Sheymov. So radio frequency, or RF weapons, are part of the pretty vast arsenal of information warfare measures. I think it's important to distinguish where they belong in that wide spectrum.

There are two different types of attacks on a computer, principal types.

One is so-called software attack. It's hacking, cracking, all those activities recently attracting pretty good attention. And another part is so-called back-door attack, which is done through radio frequency emanations from outside to the computer.

So this is attack not through the legitimate gateways of the computer. And I would like to concentrate on that.

Within that class of weapons, there are principally two parts. One is high-energy radio frequency weapons and low-energy radio frequency weapons.

High energy is a highly specialized field and it's really the latest achievements in technology. And those were covered pretty well in your February hearing. So I don't want to repeat certain things stated then.

Low-energy, or LERF, radio frequency weapons, represent a much less sophisticated technology achievement. And maybe that reflects the danger of those weapons because they don't correlate in people's minds with the latest achievements, thinking, oh, gee, somebody has to be very sophisticated.

Now, there are two principles upon which these weapons are based.

High-energy weapons need to achieve a high concentration of radio-magnetic waves or high-frequency within time, space, and spectrum.

Low-energy weapons spreads that energy over a wide spectrum of frequencies.

People usually look at the reaction of the military. The military is not quite jumping at acquiring these weapons for a very simple reason – because the military has very high standards for accuracy. At least the civilized military.

In particular, low-energy radio frequency weapons inherently do not have high accuracy. As a matter of fact, they are notoriously inaccurate, which leads to an enormously high rate of collateral damage.

However, the flip side of that is that terrorists usually are exactly after that, exactly after collateral damage. So it appears to be almost an ideal weapon for terrorists.

These effect of these weapons on computers is probably no less damaging than high energy. The radius is a little smaller, but a mile and a half is a sufficient radius for use.

So what happens, in effect, just to explain the physics of the process, there are so many frequencies in the spectrum of low-energy weapons that there will be at least one which is damaging to this particular computer.

That's the basis of that.

When I work at the KGB, low-energy weapons were worked on for different applications. But one specifically dangerous device was developed and it had a devastating effect in about a mile radius, or a mile and a half on the electronic equipment – all the TV sets went off and all that.

So it is very easy to make. The cost is under $100. The components could be bought at any electrical store. And the only obstacle between the terrorists and the weapon is know-how because know-how is a sophisticated thing.

But once somebody knows how to make it, then it could be virtually mass production or on the Internet.

There are a number of scientists and engineers in the Soviet Union who are well familiar with this technology, where the Soviet Union was the technological leader in the world. And some of these scientists are now sometimes literally hungry. They're in a desperate situation.

On the other hand, we have quite a lot of money available to terrorist groups all around the world.

I think that relying on these two potentially explosive components not coming together is less than wise policy. They can come together at any time.

We also have to realize that to design and develop effective protection against these weapons would probably take at least two years from the state where we are right now.

To design and use low-energy radio frequency weapons could take a week, travel included.

So I think we are in a dangerous situation and particularly in regard to our infrastructure.

In the press and public discussions, I have often seen and heard statements that we don't have sufficient evidence of radio frequency weapons use in the United States or against the United States.

Well, first of all, I don't find it sufficient arguments. We don't have compelling evidence of nuclear weapons used against this country yet, but, still, we're doing something about that. So why not radio frequency?

And secondly, the premise under those kinds of statements is simply incorrect because radio frequency weapons have been used in the Soviet Union and by the Soviet Union more than once. Several examples of that are available.

In 1968, during the invasion of Czechoslovakia, the resistance groups were relying on radio transmitters and radio receivers.

The Soviet air force used jammers based in the Western Ukraine and during the invasion, they were circling two airplanes consistently over the area of Czechoslovakia, effectively putting out of business every receiver, while at the same time the Soviet army was using very narrow windows in the spectrum for their own communications.

It worked very effectively.

Another example of radio frequency weapons used was the KGB use against the American embassy in Moscow.

During an operation directed at the American embassy, when the U.S. Marines were targeted, those that were guarding the embassy, which resulted in a pretty high-level investigation.

On the initial stage for destabilization of the Marines, the KGB was manipulating the American security system of the embassy using radio frequency weapons, just turning it at will, causing false alarms. The Marines are up and running, doing it several times during the night, trying to annoy and fatigue the Marines.

Another example of the use of radio frequency weapons, again by the KGB, was use against a piece of equipment in a special equipment room in the embassy, where, again, with the use of radio frequency weapons, that piece of equipment was caused to catch fire.

It did catch fire and fire spread over a sensitive area and the KGB was trying to infiltrate, bugging officers or technical experts to get into the sensitive area of the American embassy.

A very similar situation happened with the British embassy in Moscow a little bit earlier.

So, at least these are offhand examples of radio frequency weapons used and it is undoubtedly a successful operation.

Now the impact of low-energy radio frequency weapons on computers.

That impact is actually devastating. While not destroying the elements of the computer at all, it actually causes malfunction.

One of the worst parts of it is that the malfunction is absolutely impossible to predict. There are billions of combinations probably of different malfunctions. And the computer goes into so-called random output mode, which is an extremely dangerous thing.

If you just turned the computer off, that would be a relatively safe situation. When, instead, you can make a computer giving random commands.

If that computer, let's suppose, commands an aircraft, that aircraft becomes uncontrollable, totally uncontrollable. Or that computer controls, let's say, energy distribution.

The worsening factor here is also that the redundancy, which is a fairly expensive means of providing safety and security of operations in many areas, absolutely doesn't work in this area because no matter, you can put five computers or six computers redundant to each other, they all will go in random output mode.

And that is just the primary effect on the computer or computer network.

There is a secondary impact which Mr. Vadis of the FBI was discussing in February.

However, there is yet another application of that weapon which can be used in conjunction with another type of weapon.

One of the weaknesses, as far as I understand, of structures of the society here or other structures of the protective services, is that rescue operations and response teams for biological weapons, chemical weapons, explosives, are themselves using computers. And they have to get to the point of impact of the primary weapon, which means that a primary weapon, whichever nature of it is used, and then radio frequency weapon is used, then D.C. traffic would be put totally out of business and the rescue teams would have a very difficult time responding to the call.

And also, rescue teams may lose their own computers, which would be a very serious impact on the situation.

So the terrorist applications of this radio frequency weapons can go on and on and virtually every part of critical infrastructure is subject to that.

Financial markets are an addition.

For instance, estimates on just the loss of business, not physical equipment. When the IRA blew up the exchange in London, it was about $3 billion.

I'd like to take one minute, Mr. Chairman, if I may, to allude to the intelligence side of the RF operations, intercept or eavesdropping.

The KGB was very successful in that.

Now, the simple fact of life is that part of the directorate is privatized. The most successful officers and most advanced experts left for private industry.

Allegedly, several companies market their protective services to Russian banks and financial institutions, which I would call it probably part of their business. What these people do best is intercept information.

The potential for intercept and use of commercial information intercept is enormous.

For instance, proprietary mergers, advanced information, insider trading, commodities reports, and all these things, can be easily intercepted and the market could be manipulated by the clients of these companies.

Furthermore, these companies provide some of the byproduct to the Soviet government – I'm sorry – to the Russian government, which is very much interested in technological issues and commercial issues.

In exchange, these companies have full access to the pool of officers currently employed, to equipment of the government, which is extremely sophisticated, and to the facilities, including on Cuba.

So these companies could use, including the government, of course, could use those for interception of information from the United States.

And I'm not talking about information intercepted from Moscow, from private offices of American companies, and information intercepted in New York, which is very easy to do. You need a couple of suitcases of equipment to virtually have a duplicate of anybody's computer, let's say, across the street.

Altogether, these technologies, and these are flip sides of the same RF technology, whether you're receiving or whether you're jamming the computer.

So it looks like we really need to develop a strategy for development of protective technology for United States computers against low-energy radio frequency weapons.

To my mind, the ultimate responsibility for overall technology code direction belongs to the United States Congress. And I would like to thank you again for inviting me and giving me a chance to share my thoughts on the problem.

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

Representative Saxton. Thank you very much, Mr. Sheymov. We greatly appreciate you being here.

I trust you'll be able to stay for a little while because several Members will undoubtedly have some questions for you.

Thank you.

Mr. Alibek?

OPENING STATEMENT OF KENNETH ALIBEK, PROGRAM MANAGER, BATTELLE MEMORIAL INSTITUTE

Mr. Alibek. Thank you. Mr. Chairman, and Members of the Committee, thank you for the opportunity to discuss the issues of biological weapons and biological terrorism with you.

I am in a rather unique position to discuss these issues, since I developed biological weapons for the Soviet Union.

For most of my career in the Soviet Union, I was strongly convinced that we were doing the right thing in developing biological weapons. We believed that the United States had a similar program.

However, in the last few years I spent there, I began to suspect that this was not the case. My suspicions were confirmed when I traveled to the United States in 1991 as part of the Soviet Union's inspection team for the trilateral inspections between the United States, the Soviet Union and The United Kingdom.

At that point, I came to the conclusion that biological weapons must be eliminated and I left the biological weapons program.

Biological weapons are relatively inexpensive and easy to produce. Although, the most sophisticated and efficient versions require considerable equipment and scientific expertise, primitive versions can be produced in a small area with minimal equipment by someone with limited training.

The Soviet Union has the oldest biological weapons program. It was begun in the late 1920s.

Although the Soviet Union was a party to the 1972 Biological and Toxin Weapons Convention, it continued a high-intensity program to develop and produce biological weapons through at least the early 1990s.

Hundreds of tons of anthrax weapon formulation was stockpiled, along with dozens of tons of smallpox and plague. The total production capacity of all of the facilities involved was many hundreds of tons of various agents annually.

The program also included molecular biology and genetic engineering research. This research was intended to develop antibiotic-resistant and immuno-suppressive strains and to create genetically combined strains of various viruses.

The Soviet biological weapons program was the most sophisticated program in the world by far.

After the collapse of the Soviet Union, in early 1992, Russian president Boris Yeltsin signed a decree banning all biological weapons-related activity. Considerable downsizing in this area did indeed occur, including the destruction of existing biological weapons stockpiles.

Certainly, now that the Cold War is over and the United States-Russia relations have changed markedly for the better, Russia presents far less of a military threat to the United States.

However, it would not be prudent to consider that Russia presents no military threat whatsoever.

In addition, biological weapons technology can possibly proliferate from Russia to other countries less friendly to the United States, including those known to sponsor terrorism.

For these reasons, it's important that we continue to analyze the situation with biological weapons in Russia.

There are three main reasons that I am concerned about possible biological weapons research and development in Russia today.

The first reason is that many of Russia's former biological weapons facilities at Sergiyev Posad, Kirov, Yekaterinburg, and Strizhi have never been subjected to international inspections.

The second reason is that Russia continues to deny the size and even existence of many aspects of its former biological weapons program.

The 1996 annual report to the United States Arms Control and Disarmament Agency states that, "The Russian Federation's 1993-1996 BWC data declarations contained no new information and its 1992 declaration was incomplete and misleading in certain areas."

Until the Russians have provided a complete accounting of their past biological weapons activities, however, it is very difficult to believe that they have ceased all of these activities.

I have recently seen in the Russian press renewed denials of the anthrax-related deaths in Sverdlovsk in 1979. But the world already knows that these deaths were the result of an accidental release from the biological weapons production facility there.

Third, among the Russian scientists' published work, there are many studies that I feel are dubious or even outright offensive biological weapons work.

There are numerous ways in which Russia's biological weapons expertise can be proliferated to other countries. The most obvious is the departure of Russian experts to other countries.

I have contacts in the United States who maintain connections with these Russian scientists, and through these contacts I have learned of the pitiful state of these experts. Many of the scientists are underemployed or unemployed.

It is therefore not surprising that some of them would seek to emigrate.

A second possibility of proliferation is the sale of technology or equipment to other countries, either by the Russian government or by some scientists.

There were allegations in a February 12th *Washington Post* article of negotiations between the Russians and the Iraqis for sale of fermenters allegedly designed for single-cell protein production, used for animal fodder.

And there is no doubt in my mind that these fermenters were designed for use in biological weapons production.

First of all, Iraq has used this explanation as a cover for biological weapons facilities in the past.

Second, the particular fermenter size involved in this proposed sale would not be suitable for efficient single-cell protein production. In fact, the resultant product would be prohibitively expensive.

As an example of the sale of technology by some scientists, I have a copy of a flier advertising the wares of a company called BIOEFFECT Ltd., with offices in Moscow and Vienna, Austria.

It is clear from this flier that the scientists of BIOEFFECT, Ltd. are willing to sell their genetic engineering knowledge to anyone.

There is another mode of proliferation: some Russian scientific publications.

For example, a recent article detailed a method for cultivating the Marburg virus. Marburg virus is one of the most serious agents that could be used in biological weapons. This method is so simple, and requires so little equipment and training, that it could be easily adopted by a terrorist group.

Other, more sophisticated types of information concern genetic engineering methods, antibiotic-resistant strains of pathogenic micro-organisms, and so on.

While we should not ignore the continuing threat of military use of biological weapons, we are not at present poised for war with any nation known or suspected to possess biological weapons – with the possible exception of Iraq.

A more likely threat is that posed by the terrorist use of biological weapons.

There is no doubt that the potential impact of such an attack is great. A report published by the Centers for Disease Control in April of 1997 evaluated the economic impact of a bio-terrorist attack for each of three different biological agents.

Their model showed that the expected impact from such an attack would range from $477 million to $26 billion per 100,000 exposed people.

Therefore, there is no doubt that we will see future uses of biological weapons by terrorist groups, as there have been several attempts already.

Certainly, it behooves us to be prepared for biological attacks. The ultimate goal for defense is to prevent suffering and loss of life, thereby rendering biological weapons ineffective.

There have been many efforts in recent years to improve our preparedness – creating agent detection systems, developing data bases with biological weapons information, training those who would respond first to a biological attack, and so on.

However, while all these measures can potentially reduce the suffering and loss of life experienced after a biological attack, they are of limited value without an appropriate medical defense.

Only the development of appropriate medical techniques can completely eliminate the threat of biological weapons.

Vaccines of course have completely changed the picture of infectious diseases on earth. Smallpox has been eradicated. Poliomyelitis has lost its epidemiological significance. In bio-defense, vaccines can also sometimes be used as urgent prophylactic measures.

Now we mostly develop and use vaccines for bio-defense. However, vaccines have a number of limitations.

A particular vaccine works only against a single illness or occasionally, against a few similar illnesses. For many illnesses, a vaccine has not yet been developed.

Even if every illness had a vaccine, it's impossible, even dangerous, to vaccinate a person against every possible biological agent, since there are over 50 such agents.

It is also unrealistic and prohibitively expensive to vaccinate every person in the United States against even a few agents.

Vaccines are, therefore, most useful and economical as bio-defense when we can limit the possible agents to a few and when we know who the specific target population is.

This generally means that vaccines are best used in troops at the front lines against an enemy whose biological agents of choice are known to our intelligence.

Again, vaccines do not exist for every known agent and existing vaccines might not work against genetically altered agents.

Clearly, in most military and terrorist attacks with biological weapons, vaccines would be of limited use. Therefore, we cannot rely exclusively or even primarily on vaccination for medical bio-defense.

We must also ensure that means for urgent prophylaxis and treatment of these diseases are available as well.

I feel strongly that we must devote additional resources to the medical aspects of bio-defense. As part of this medical research, we must consider a new approach – fundamental research and development of methods for nonspecific defense.

This type of defense is based on amplifying the immune response of the human body to invasion by any foreign agent.

This medical research and development will pay for itself many times over.

In addition to contribution to our nation's preparedness for biological attack, it will provide a much-needed push in the treatment of infectious diseases that occur under natural conditions.

Infectious diseases remain one of the leading causes of death in the world and cause tremendous losses in terms of both money and human lives every year.

Furthermore, this research, especially that into nonspecific defense, will also contribute to the treatment of many other types of diseases, such as auto-immune disorders and cancer.

One possibility to significantly increase research in this area would be to establish a medical research center specifically for this purpose.

Such a medical research center would also provide one option for addressing certain non-proliferation concerns. The center could employ Russian scientists who participated in the development of biological weapons and are currently under- or unemployed, to conduct medical research for the United States bio-defense program.

In this way, we can ensure that the knowledge of these "graduates" of the most sophisticated biological weapons program in the world is put to peaceful use, and we stand to reap the benefits of their extensive experience.

Another important aspect of our bio-defense program is the continuous analysis of possible routes for biological weapons development in other countries. This analysis must cover everything from new biological agents to new delivery means.

The focus of such analysis is to identify the threat as clearly as possible in order to focus our medical research and other bio-defense efforts as accurately as possible.

We can thereby avoid wasting time and resources developing defense against a nonexistent threat.

Finally, several more areas require our continued attention to round out our readiness for biological attack.

Creation of manuals for those who will respond to bio-terrorism incidents.

Revision of existing manuals for military physicians.

Creation of practical means for defense against possible unusual variants of biological weapons.

Addressing these requirements – medical research, threat analysis, manual revision, and defense against unusual biological weapons variants – will greatly enhance the United States' preparedness for a biological attack.

Thank you.

[The prepared statement of Mr. Alibek and the accompanying study appear in the Submissions for the Record.]

Representative Saxton. Thank you very much Mr. Alibek.

Mr. Fairchild. For those of you who didn't hear Mr. Fairchild's introduction, he's a former Green Beret, retired from the CIA, with a great deal of experience in his latter career.

Mr. Fairchild.

OPENING STATEMENT OF BRIAN P. FAIRCHILD, BRIAN P. FAIRCHILD AND ASSOCIATES

Mr. Fairchild. Mr. Chairman, Members of the Committee, thank you very much for inviting me here today to testify on the state of our country's clandestine service. As you know, I was a career staff officer for the CIA's directorate of operations, the DO, and I am proud to have served in this capacity.

I found my career with the CIA fascinating and enjoyable. I had very memorable experiences, and if I had it all to do over again, I'd take the same path.

Let me state at the outset, Mr. Chairman, that the United States needs a strong and dynamic DO, which can collect human intelligence on select strategic intelligence topics that are so important to our policy-makers.

As my fellow panelists have just explained, our country currently faces serious external threats. Chemical, biological, and nuclear weapons are among these threats, as are threats to our strategic industries through industrial espionage.

In addition, the United States continues to be plagued by terrorism and international crime.

Economically, these threats represent potential economic disaster if they should befall us.

An attack on our country by weapons of mass destruction would result in the loss of billions of dollars, and the cost of international crime is already estimated to be in the hundreds of millions.

Moreover, the impact of industrial espionage could eventually prove fatal to our strategic industries.

The DO is our nation's first line of defense against these threats and, as such, it cannot afford to be second best. Unfortunately, the DO has a number of systemic problems that must be addressed if it is to make a successful transition into the next century.

One problem the DO has is external.

Its reporting scope has been vastly expanded from what it was intended to be. The DO was intended to obtain only that information which had to be gathered through espionage. And, its original customer base was the President of the United States and the National Security Council.

Now, the DO has numerous customers, including almost all government departments and agencies and every year, these customers task the DO with an increasing number of requirements, the majority of which could and should be serviced by other agencies.

Now, this dilutes the DO's capabilities and ensures it will be unsuccessful in its efforts to focus on the most pressing and vital intelligence topics in the future.

As you know, Mr. Chairman, the DO's primary responsibility is to recruit human sources. And when these sources are well placed, they can provide information critical to the policy-makers.

Now, I don't mean to imply that technical intelligence, such as signals intelligence or satellite photography, is of no value. On the contrary, it often makes a unique and valuable contribution.

But there are vital areas that only human sources can cover.

Therefore, the DO must continue to aggressively recruit these sources, and it has some remarkable case officers who can carry out this mission.

The recruitment of sources, however, is not the only mission that the DO has. The DO is also charged to ensure that its officers are well covered overseas, and it is charged to maintain a vigorous counter-intelligence and operational security capability.

Unfortunately, the DO has not done a very good job when it comes to cover, counter-intelligence, and operational security. This is a serious problem because recruitment operations that are pursued by case officers with poor cover, and without the benefit of a counter-intelligence program, and good operational security, what the CIA calls "tradecraft," are very likely to become compromised.

What does that mean, if an operation becomes compromised?

This means that our foreign sources can be arrested. Our officers can be kicked out of the countries, persona non grata. Our sources can be quietly transferred out of positions in which he or she had access to classified information. The operation can be monitored by the counter-intelligence service to determine our method of operation and to identify additional officers.

But worse, if an operation is compromised, the asset can be turned against us as a double-agent, and used as a channel for disinformation to our policy-makers.

Simply stated, counter-intelligence and good tradecraft are just not part of our case officers' professional lives.

The reasons that counter-intelligence and operational security are not part of our case officers' professional lives are rooted in the history of the Cold War, which I detail in my written statement, and I won't go into now, Mr. Chairman. But another reason is because the DO emphasizes recruitment over all else.

The DO only has one career track, that of recruiter and all case officers are forced into that mode.

The single career track system is the cause of limited promotions between grades, and this has caused much dissatisfaction within the officer corps.

The limited chance for career advancement in the DO has led to a unique phenomenon – the exodus of junior officers, many of whom have resigned while on their first tour of duty overseas. This is obviously a major problem for which a solution must be found.

As serious as these problems are, they can be fixed.

The President, the National Security Council, and the Congress, working together, can once again limit the DO's reporting scope to only that information which must be obtained, at risk, through espionage.

New cover mechanisms can and must be developed for the majority of case officers overseas, although a few will always be required to stay in the embassies in order to have access to official targets.

It's also time for the DO to recognize that there are no benign operational environments overseas, and to provide in-depth tradecraft training to all of its officers. This training should be the foundation on which all officers build their careers.

The DO must emphasize the importance of recruiting sources within local counter-intelligence services. This is the keystone for all successful operations.

And the DO must open new career tracks in counter-intelligence, operational security and agent handling which will not only provide more avenues for career advancement, but will make all DO operations more secure and less prone to compromise.

Finally, Mr. Chairman, as the system stands today, all case officers are generalist recruiters. As such, the DO has few officers who are proficient in languages and who specialize in geographical regions.

Although there are a small number of case officers who can recruit anywhere any time, with little language and little area familiarization, in the main, language skills and area familiarization are sorely needed in the DO and the DO should encourage and reward officers, no matter what career track, for developing these skills.

As brief as it is, Mr. Chairman, that's my opening statement, and thank you very much for inviting me here again.

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

Representative Saxton. Mr. Fairchild, thank you very much.

I will lead off the questioning here and we'll go back to Mr. Sheymov.

Sir, you mentioned the term, privatization, with regard to activities being pursued in Russia. Can you explain further what type of privatization activities are underway within, particularly, former KGB personalities, what types of activities they're involved in, and whether those activities at this point have gone beyond the bounds of the former Soviet Union?

Mr. Sheymov. Yes. What actually happened, the KGB went through restructuring after the 1991 period. And the KGB was in several independent agencies where 16th and 8th chief directorate comprised the new FAPSI organization, which is the Russian acronym for the agency for government information and communications security.

Several senior officers of these agencies retired. But having retired, they obtained some of the equipment, quote, unquote, no longer needed,

which was, incidentally, of extremely high quality. And they took away the best brains in both directorates.

Now what happened, they set up private companies with an extremely good base, technologically, an extremely good base in terms of personnel and talent, and somehow, they appeared to have a lot of money to do that.

So they started catering to clients, primarily focusing on operations in Moscow.

I'd like to avoid going publicly into naming the companies and naming certain activities, but let me say it's highly likely that their travel or their personnel travel abroad could be related to collection activities of at least commercial information and financially-sensitive information.

Needless to say, they do that virtually with impunity in Moscow on officers of any American company based there. And through their computer networks, they can go anywhere.

So I think that's basically the situation.

However, the important point here is that the pay of the privatized companies, or earnings of individuals working there, is much, much higher than anybody could possibly dream of in the FAPSI, in the government.

So, it becomes a very attractive alternative, like golden parachutes, for people who currently work for the government. And they maintain close ties, which were traditional in the first place, but reinforced by financial interests.

So every one of the people working for the government is dreaming to get to those private companies when their time comes. Not necessarily retirement. It could be in the middle of their career. Just a matter of being good enough professionally and accommodate those people to get on board and get paid many times higher.

So they would go, obviously, out of their way to provide information from the government, new technological developments, equipment exchange and, ultimately, the powerful facilities would be available to these companies, directly or indirectly.

Representative Saxton. Well, thank you very much.

As I was asking Mr. Sheymov the question, we were fortunately joined by our fourth witness, Mr. Nick Eftimiades. Just let me review once again who Mr. Eftimiades is.

He's here today to discuss, at least in part, the contents of his book, *Chinese Intelligence Operations*, which is considered to be the first ever

scholarly analysis of the subject which has been translated into four languages.

He has also held positions with the CIA. He has written numerous articles and a monograph entitled, "China's Ministry of State Security – Coming Of Age In the International Arena."

He graduated from George Washington University with a BA in East Asian Studies and a Master's in strategic intelligence.

We'd be anxious to hear in the next six or eight minutes your testimony, sir.

OPENING STATEMENT OF NICHOLAS EFTIMIADES, AUTHOR OF *CHINESE INTELLIGENCE OPERATIONS*

Mr. Eftimiades. Thank you, Mr. Chairman, Committee Members.

I'd like to thank you for the opportunity to speak before the Committee today. And I need to emphasize, first, that I am a senior intelligence officer for the Defense Intelligence Agency, that I am speaking today as a private citizen and as an author and not as a representative of that agency or the U.S. Government.

The issue that I'm here to speak about today is one that I believe is critical to America's national security and economic well-being.

That being China's clandestine intelligence operations in the United States and targeted against U.S. businesses, the political apparatus and military and technology industrial infrastructures.

The operational methods of China's intelligence services aren't anything new to espionage. They are, however, uniquely Chinese in their application.

The two major entities involved in that – the ministry of state security, China's premier civilian intelligence agency, and the People's Liberation Army Second Department, which is under the general staff department, recruit vast numbers of travelers coming to the United States, studying in the United States, to conduct, quote, economic espionage or illegal technology transfer.

Those entities and others also have very aggressive recruitment programs targeted against foreigners visiting China. In particular, very aggressive technical surveillance operations, which I'll go into just briefly.

To give you some type of scope in picturing this or understanding it, the expansion of Chinese intelligence operations specifically targeted against U.S. technology have grown to the point where I guess in the early to mid-1990s, the U.S. Customs Service announced that approx-

imately 50 percent of the 900 technology transfer cases they investigate on the West coast annually deal with the People's Republic of China.

So that gives you an idea of the breadth of how big a scope of Chinese intelligence is occurring.

By and large, particularly in the area of technology, the bulk of the operations are targeted against mid-level technology. The reason being for this is that China's industrial infrastructure, its technological-industrial infrastructure is 10 to 15 years behind that of the United States.

So, person for person, for any number of operations, the vast majority of those are targeted against lower levels of technology. And as a result, of course, there's less of an interest on the part of U.S. law enforcement or intelligence or prosecutors to pursue those crimes.

The only time we really hear about it is cases when we have relatively high technology and national security related technology, which come to the forefront in the press.

Just to be clear at this point, when I speak of China's illegal technology transfers, we're talking about the modernization across the board of an entire society. And this isn't something that's very specifically limited to military technology.

We're talking about multiple facets of Chinese society and the industrial infrastructure modernizing in part through the illegal acquisition of U.S. technology and trade secrets. And the intelligence services are one major player in helping those entities, private and government, in China acquire that type of data.

In extreme cases, the PRC has even been known to attempt to purchase U.S. firms for access to technology.

In the early '90s, we had the U.S. order China to divest itself of MAMCO. The China National Aviation Technology Import-Export Corporation has purchased the U.S. company, MAMCO, with the attempt to trying to get access to in-flight refueling technology.

We caught it at that time and asked them to divest themselves of the company.

But those types of operations are pretty high profile and it doesn't fit a normal operating pattern with Chinese intelligence, which is one of three.

Usually, U.S. firms who are conducting joint ventures with Chinese firms are subject to intelligence activities levied against them.

Two, is just to recruit assets who are coming over to the U.S. and studying long-term programs as scholars or scientists and the Chinese, in

fact, intelligence has a slang term for that – chundiyoo – fish on the bottom of the ocean, in which they recruit people and place them in the U.S. in high tech fields, knowing that they're not going to use them for five to 10 years.

And I got the opportunity, actually, of debriefing a number of people who were in this position and who had gone through this training, were recruited for that purpose.

And third, the third method of operation that they use is a pretty common one for them, which is using individuals in front or cover companies, primarily out of Hong Kong, or a lot out of Hong Kong, to try and get access to U.S. technology that way.

In addition to China's activities in the United States, they also run a very aggressive domestic intelligence program. That is, a program designed tc try and collect information visiting officials, business persons, scholars, technicians, et cetera.

And it's not just the intelligence service involved with this. China's intelligence services count on estate ministries, people's friendship societies, academic institutions, and entities in the military industrial complex to assist them in recruitment, information operations, collection operations to provide cover to operatives, et cetera.

Technical surveillance. Technical surveillance is also very aggressive in the PRC. A number of hotels, the Palace Hotel, the Great Wall Hotel, the Xiang Shan Hotel, some of the premier hotels in Bejing are technically monitored, specifically targeted for visiting officials and businessmen.

And the intelligence services obviously exploit that.

One thing to be wary of, as I look at China and their domestic operations targeted against U.S. officials, is that not only do they have the technical surveillance that's conducted normally for your visiting persons, but picturing the scale here, some time ago the ministry of post and telecommunications estimated that it intercepted 26 percent of the international calls dealing with Chinese citizens.

Now think about that for a second – what it must take, how much manpower you have to put in to intercept 26 percent of a society's international calls.

It's just incredible the amount of manpower that's thrown at the problem. The ministry of public security again intercepts well, well in excess of that, probably in the 60 to 70 percent range of incoming mail.

So China's intelligence programming conclusion is extensive. It's very, very well targeted. It's across the board. And it's, for all intents and purposes, unaddressed.

Thank you very much.

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

Representative Saxton. Mr. Eftimiades, based on what you've said, it's very obvious that you're extremely familiar with these matters and that you're undoubtedly familiar with an article that appeared in *The New York Times* on May 16th, authored by Jeff Gerth.

I'm not going to ask you about the specifics of the article or the related matters. However, I would like to ask you if this appears to be part, or could be part, of a regular pattern of activities carried out by foreign governments, particularly the Chinese.

Mr. Eftimiades. Well, first let me say, I appreciate your not asking the specifics of that.

However, as far as a general pattern goes, and a very serious note, sir, if we're looking at bribing foreign officials, if that is the process that the intelligence service uses, I've got to say, for China, that's the norm.

It is an absolute norm.

We cannot look at this with American eyes on. We are dealing with a culture, a 3000-year-old culture, that has essentially been rule of man. Not rule of law.

It's only in recent years that the National People's Congress has even started to step to the plate, as any type of respected legislative body, and rule of man is the case in China.

And that being the case, this is common practice. It's common practice in business activities. It's common practice in intelligence activities.

So to answer your question, sir, it fits a very, very common pattern.

Representative Saxton. Can you elaborate on the process used by the Chinese to put people in key positions to penetrate U.S. and other countries' political operations?

Mr. Eftimiades. Yes, sir. In fact, let me quote a while ago in a case in Norfolk. Some files became public, one of which were the words of China's chief of North American operations.

And he said to the recruited asset that he had – your primary objectives are the White House, the Congress, and Washington think tanks.

If you're not working against those targets, then don't bother with it. So we clearly see intent on the part of China's intelligence services.

As for methodologies, the process – there are two basic types of agents that are recruited. A long-term agent, a sleeper, as I described, and short-term agents.

The long-term agents are routinely recruited six, eight, nine, ten months as a recruitment process. These people are vetted very aggressively, psychologically studied for people who are going to be traveling to the United States for business or for long-term advanced degrees in studies.

The persons are given some, after psychological assessments are done and the recruitment process, lots of questions. The person is eventually given training, usually several weeks of training, given cash sums, some means of clandestine communications.

And this is a characteristic pattern that I see in these types of operations – means of clandestine communications with China, security, lectures on the U.S. Congress, lectures on our system of government, lectures on our media, an entire training program.

The person is deployed.

They keep in touch through writing to accommodation addresses every two to three months. They're met person to person by their handlers every two years or so in a third country. And these persons are basically kept, as we would say, on ice for five to 10 years.

And that's what they're told – you're not going to do any operational activity for five to 10 years. Get to know people, people who you think are going to be prominent, people who are moving up, people who are aggressive.

So they sit that with as an incubation period. And it's cheap. It's cheap for them. It's an absolute cheap way of deploying people if you have the patience to exploit those contacts five to ten years later.

Representative Saxton. Mr. Alibek, if I may back up to you just a minute and then we'll move on to the other witnesses for some questions.

How large is the current biological weapons program in Russia? How many people work there, just to give us some idea of the scope of what may be happening there?

Mr. Alibek. If to say about the Soviet Union's program, it was a deliberately huge and sophisticated program, about 60,000, 70,000 people, just in developing biological weapons in Russia, several main directorates.

Now we can say two of three main directorates were eliminated by serious efforts from the United States and the international community.

For example, the civilian arm of this defensive program is not a threat any more. The agricultural department is not a threat any more.

But the most serious concern is the main directorate on chemical, biological and nuclear defense and its biological part.

It manages four facilities. They down-sized recently. But they conduct work in this area and in my opinion, several thousand scientists and engineers are working there.

I can say now – I'd like to say that Russia doesn't have biological weapons stockpiled now. But Russia does have very serious scientific potential. It tries to maintain its biological and technological potential and tries to keep some production facilities just so it could be ready for possible exploitation in the future, to be used in the future.

Representative Saxton. When I asked Mr. Sheymov about the export of radio frequency technology and the propensity of other countries to make use of technologies developed by the former Soviet Union personnel, I assume that if I ask you the question, you would say it's relatively easy to export biological weapons technology.

Is that true?

Mr. Alibek. That's absolutely right. In my opinion, there are many ways for transfer.

I mentioned the possible emigration of the scientists overseas or abroad. For example, just as an example, about 20 scientists who were involved in developing biological weapons in the Soviet Union had a chance to emigrate to the United States.

They are not involved in any offensive work here because this country doesn't have this offensive program. But this is just an example. It's not a problem for the scientists to emigrate and a lot of them are here in the United States. We can assume some of them, of course, could go to Iran, Iraq, and some other countries.

Technology transfer, equipment selling, dual-purpose equipment sale, as we saw with Iraq.

A couple of new examples of Iran activity in this area. They sent a group of scientists just to understand what's going on, just to get some knowledge in this area.

Russia now is conducting negotiations to sell equipment to manufacture antibiotics to Iran. In my opinion, it's clearly dual-purpose equipment. It could be used for manufacturing biological weapons.

Some scientists try just to advertise their knowledge. The most serious problem, as I said before, a lot of under-employed and unemployed Russian scientists, thousands and thousands of them are now unemployed.

I've talked to them and you know what I heard? One of them told me, it doesn't matter who pays because you know, I've got children. I've got my family. If I am paid, I will do this work.

That's the problem. And we need to realize, of course, it's a serious problem and we need to do something with that.

Representative Saxton. Let me ask you one rather specific question relative to North Korea and South Korea and our forces that are in South Korea.

I have reason to believe that North Korea has developed or has imported Russian technology, Soviet technology, in this area. If you would comment on that.

And also, whether you have been called upon by officials in the United States to help develop or provide information that would help us with ways to combat what may exist in North Korea in the way of antidotes, et cetera.

Mr. Alibek. Thank you for the question. I want to say, the Soviet Union's program, offensive program, offensive biological program, was the most secret program in the former Soviet Union. Even more secret than the nuclear program.

In those days, it was impossible to sell or to share any information regarding biological weapons with any country at all.

But I know that North Korea does have an offensive program, offensive biological program.

I obtained this information just analyzing Russian intelligence sources of information. There was a program and we needed just to look through and analyze the situation with this country very carefully.

But there is another way.

It's not necessary just to sell biological weapons technology. It's possible to sell or to share general biological knowledge. It would be

enough for a country that is interested in developing biological weapons to have this equipment or to know the general technological process, to develop biological weapons on its own.

Representative Saxton. Thank you.

Mr. McCrery, would you like to take some time for some questions?

OPENING STATEMENT OF REPRESENTATIVE JIM MCCRERY

Representative McCrery. Thank you, Mr. Chairman.

Mr. Alibek, you mentioned that in 1979, the Soviet Union entered into a compact on biological weapons.

Is that correct?

Mr. Alibek. I'm sorry. Could you repeat that question?

Representative McCrery. You said that in 1979, the Soviet Union entered into a compact on biological weapons.

Mr. Alibek. I didn't say anything like that. I mentioned 1979 just in one case.

There was an accident in Sverdlovsk. That's why I mentioned 1979, the year. I said it was a case of a serious accident that occurred at a military facility at the ministry of defense that caused a lot of deaths.

And even Yeltsin in 1992 admitted that there was a case caused by the military, the Russian military.

But, unfortunately, even now, if you look through Russian newspapers, you see that some government officials say of course there was no accident. It was just a case of contaminated meat.

They use some kind of Cold War rhetoric, unfortunately, what we see now.

Representative McCrery. Thank you. Mr. Eftimiades, you mentioned in your written testimony the Chinese company, China National Aerotechnology Import and Export Corporation. You used their acronym, CATIC.

And you mentioned in your written testimony that the Bush Administration declared that this company had a checkered history.

Can you expound upon that? What was their checkered history?

Mr. Eftimiades. Yes. Actually, I can, sir.

That company – we can't think of that in terms of companies. That's an entity under the People's Liberation Army. It's as if you nationalized

every manufacturer that made jet fighter aircraft in the United States and made them all officers, and that's the company.

Up until '83, it was a ministry, and then they just changed names. So that's really what we're talking about here.

And fitting under the commission of science and technology and industry for national defense, those entities had been nailed a number of times in trying to collect illegal – actually, successfully sometimes – getting U.S. technology illegally.

So that, plus the military applications that it clearly had, I think was enough probably for the Bush Administration to say, no.

Representative McCrery. When you say the Bush Administration said, no, what do you mean?

Mr. Eftimiades. I mean divest themselves of MAMCO Company at that time. They realized the history of this company, the company's involvement in previous times.

That entire block of the military industrial entities of China have been repeatedly, since 1979– actually, as early as 1979 – that I was able to trace any number of cases where they had tried to acquire and successfully acquired technology illegally.

So I think the entire history of that, plus the military implications of CATIC gaining that access to that type of technology for in-flight refueling capabilities, forced the Bush Administration to refuse them to hold onto MAMCO as a corporate entity.

Representative McCrery. And is this the same company that Lieutenant Colonel Liu, the daughter of General Liu, is involved with as an officer?

Mr. Eftimiades. It's tough to say. The short answer is no. The long answer is there's such an intermix of that type of technology and that type of space systems.

If I remember correctly, Liu works for China Aerospace Holdings, I believe it is, China Aerospace International Holdings.

Now that company was purchased, 51 percent or so, in 1993 in Hong Kong by China Aerospace Corporation. Now China Aerospace Corporation is the one who does all the launches and the government entity that does all that. And they are inextricably linked, obviously, with China Aviation Technology Import-Export Corporation.

So it's six of one, half dozen of another.

She's still the PLA. That's the bottom line.

Representative McCrery. So, technically, she's not an officer of that particular company. But she works for a company that is inextricably linked to CATIC.

Mr. Eftimiades. Well, technically, she is a People's Liberation Army officer who is working for China Aerospace Corporation, which is an entity of the Chinese government in aerospace industries.

Now it's like civilian military aerospace, and where the linkages are and how close they are, it's impossible to say. it's not quite as clear-cut on the line and block chart as our system is.

Representative McCrery. But there is some connection.

Mr. Eftimiades. Oh, absolutely, yes.

Representative McCrery. And is CATIC the company that was involved with Loral Hughes in the launch?

Mr. Eftimiades. To be frankly honest, sir, I've got to tell you that I haven't followed the Loral Hughes issue and to see in detail who's been following what.

So I don't want to say yes when I'm not absolutely sure, and to what degree their involvement might be.

Representative McCrery. Thank you.

Representative Saxton. Senator Bennett?

OPENING STATEMENT OF SENATOR ROBERT F. BENNETT

Senator Bennett. Thank you, Mr. Chairman.

I want to thank all our panelists. I've enjoyed – well, I haven't enjoyed the information you've given us, but I've been enlightened by it and congratulate each of you for the thoroughness with which you've examined your particular areas of expertise.

Mr. Eftimiades, if I may be allowed a personal comment, you'd better be careful. In your testimony, you'll run the risk of having the Democratic National Committee accuse you of being a racist for your comments about the Chinese focusing first on Chinese nationals.

Of course, this is not the Thompson Committee, so maybe they're not following the hearings as carefully as they did some of ours.

I'd like to go back to those hearings, which is my background for raising some of these questions.

You have already answered them a good bit in your testimony. But I'd like you to use the Ben Wu case as an example and give us a specific example of how Chinese intelligence goals are met.

Mr. Eftimiades. Ben Wu was a case where – Ben was arrested in 1992, convicted in 1993, for 10 years for illegal technology transfer.

Specifically, he had already transferred second-generation night division devices for the PLA.

He was recruited in China – now I had discussed earlier a long-term agent. This was a Chinese example of a short-term agent, as they call it.

He was recruited inside China, just a few months prior to going to the United States. He had connections, I think family connections, with the computer industry in Virginia.

So he came to the United States as a recruited asset of the ministry of state security.

Somewhere along the line, he got cold feet and went to the FBI and said, hey, I'm a recruited asset by the ministry of state security.

He started working for the bureau but, alas, he double-crossed everybody and was still sending illegal devices to the ministry of state security.

It was kind of an interesting case because when they did arrest him, he had almost a half-million dollars in the bank, arrested with two others who were, I believe, students, former Chinese government officials, one student, I think, at James Madison University and I forgot where the other one was.

He was tasked against U.S. businesses and had a specific laundry list of technologies that he was supposed to go after – again, not third generation, but second generation, mid-level technologies that the PLA could incorporate easily.

So it was what I kind of term as a throw-away agent. He was short-term use, effective, and they got what they wanted from it.

Senator Bennett. Can you tell us about the relationship between Chinese criminal organizations – they used to be called tongs. I think now they're called triads – and Chinese intelligence?

Mr. Eftimiades. There hasn't been much identifiable. Those relationships are very shadowy, frequently. There have been some publications. Peter Lund, formerly of Canadian intelligence, who watched the Chinese, has published on that, having headed the Hong Kong corruption commissions for six years.

The nature of the relationship is shadowy. It's most solidified in Hong Kong. Certainly, Chinese intelligence doesn't operate there without having some association or relationship with the triads.

This came to light in the Tiannamen incident, or shortly thereafter when I think the triads were actually assisting in pulling people out of China and kind of ran afoul of some elements of Chinese intel.

As to the nature of the relationship, the depth, how it might be used as a control mechanism, I don't have the details on it, sir.

Senator Bennett. We've already made reference to the relationship between Chinese military intelligence and Johnny Chung. And you've described the Chinese military intelligence department and as I understood your testimony, the relationship with Mr. Chung was fairly typical of the kind of thing that they would do.

Is that a fair characterization?

Mr. Eftimiades. Sir, the patterns of those operations are just common. I mean, that's the way business is done.

Senator Bennett. Have you followed any of the other revelations that came out of the Thompson Committee regarding China? Do you have any comment on any of the other operatives – John Huang, Maria Hsia, some of the other names we're familiar with?

Mr. Eftimiades. I'm familiar with the names. Just the elements in the public domain as to what the process has been.

Again, if the question is, is the pattern normal? Sure. Absolutely.

Senator Bennett. I wanted to pursue that, Mr. Chairman, because we heard over and over again in the Thompson Committee that there was no pattern. Johnny Chung was dismissed as a buffoon and there was no pattern to what he did. There was nothing logical about the way the proceeded.

At the time, I saw a clear pattern and demonstration of a typical Chinese activity. That's why I've been pursuing these questions in this fashion.

Thank you, Mr. Chairman. I have no further questions.

Representative Saxton. Mr. McCrery?

Representative McCrery. Thank you, Mr. Chairman.

Mr. Alibek, I want to follow up on my initial question. I got the date wrong. It was the 1972 convention. And the Soviet Union was a party to that biological and toxin weapons convention.

I think in your testimony you say, basically, the Soviet Union ignored the convention that they signed on to, and not only did not dismantle their program, but further intensified their efforts to develop offensive biological weapons.

Is that correct?

Mr. Alibek. That's correct. In 1972, the Soviet Union signed the convention.

In 1973, the Soviet government signed a top secret decree to intensify all works in the area of research and development in manufacturing biological weapons.

Representative McCrery. And that top secret directive was contrary to the provisions of the public convention that they signed?

Mr. Alibek. Absolutely different. Of course, you can imagine that that decree said that this program has to be completely new, sophisticated program involving genetically-altered agents, more efficient agents for manufacturing biological weapons, delivery means, production capabilities, new stockpiles and creation of new organizational capacity.

As a result of that secret decree, by the beginning of the '80s, and in the '80s, the Soviet Union's offensive program became the most sophisticated, most powerful in the amount of agents that could be used in future wars.

The amount of weapons was just enormous.

Representative McCrery. Thank you, Mr. Chairman.

Representative Saxton. Mr. Fairchild, in your testimony, and I just want to make sure that we understand what it is that you are getting to here, you talked about CIA resources being devoted primarily to recruitment.

I think you said that viable cover for our assets is, and I quote, "non existent."

Mr. Fairchild. Yes.

Representative Saxton. Is that correct?

Mr. Fairchild. Yes, Mr. Chairman.

Representative Saxton. That's unbelievable to me. Would you elaborate on that?

Mr. Fairchild. Well, Mr. Chairman, the majority of our case officers overseas are covered in embassies. And this is a result of an historical situation where after World War II, the world was in a shambles. We emerged from the war the strongest country in the world. And the Cold War was initiated.

In an attempt to fight against the Soviet Union, we established stations in countries all around the world in order to fight the Soviet target.

Now, that made sense at that time, because at that time, the majority of the world was either decimated or underdeveloped and there was no commercial entity or commercial representation in many of these countries in the Third World.

So it was logical to put our officers, for protection purposes, as well as for cover for status, into embassies.

And then we dealt with the security services in those countries and trained and equipped them in order to fight the Soviet target.

At some point in history, however, the countries that we had helped started turning against us – their policies, their military, economic and diplomatic policies started to differ from our policies.

And at that point, the services that we had been working so closely with started looking at the U.S. presence, at U.S. intelligence operations.

Now, what we in effect did in putting our stations and our officers in embassies, we effectively stuck a flag in the sand and we told the counter-intelligence services of the world, here's where we are. If you want to find us, look here.

Now, that puts us at an immediate disadvantage because the counter-intelligence services of those countries don't have to look at 150 different entities or 5,000 entities or whatever. They have to look at one location.

To make matters worse, we invited foreign service nationals, the local citizens of those countries, into our embassies as employees, many of whom staff very important positions in all the different sections of the embassy.

There is no way that you can maintain a cover for an officer in an environment like that, especially when you have a DO that is very aggressive in going out and making recruitments.

So what you come down to is you've got a situation where staff officers of the local counter-intelligence services can actually become employed in the embassy.

We have a policy where, when things need to be repaired in the stations overseas, the case officers have to leave and local employees are escorted into those spaces in order to do repairs.

So, in this kind of a situation, it's very difficult to maintain cover.

Representative Saxton. We have a technological problem here. Our beepers have stopped working. I don't know if that's a result of—

(Laughter)

—and we're expecting a vote on the other side of the Capitol.

Senator Bennett. Y2K problem.

(Laughter)

Representative Saxton. It must be. So we're trying to communicate here to find out what's going on on the other side of the House just temporarily.

But, in any event—

Senator Bennett. Mr. Chairman, may I follow up on your question here?

Representative Saxton. Sure.

Senator Bennett. You may not be aware that I have a history in this area. I'm willing to disclose it because my opponent in the Senate race disclosed it and did everything he could to make it sound terrible.

But a company that I owned provided cover for CIA agents in both Europe and Asia and was recruited by the CIA to do that for the very reason you've described, Mr. Fairchild.

Mr. Fairchild. Yes.

Senator Bennett. It turns out there was a high-ranking officer of the KGB who wanted to defect and said, I will not defect to the CIA people in the embassy because it will be instantly known that I have done that.

And so, the CIA asked my firm if we would set up a branch office in a Scandinavian country. They set up an export-import business, staffed it with CIA officers. The KGB colonel, I believe it was, defected to them. He was then taken to Mexico City for his debriefing, where my company set up another branch office.

This is the comment I want to make as to the dilemma you've described.

That was all done before I bought the company. After I bought the company, I allowed the cover relationship to

continue.

But it was done in the '50s, at a time when it was assumed by every American that it was his or her patriotic duty to cooperate with the CIA in this fashion.

The Washington Post would give a business card that would say, Reporter, *The Washington Post*, to a CIA officer and feel that it was fulfilling its patriotic duty.

The New York Times would provide cover for people overseas.

As I say, when I ran for the Senate in 1992, the fact that I had participated in this type of activity and allowed my company name to be used as cover for CIA officers overseas was raised by my opponent as a demonstration of how sinister I was.

And instead of it being an act of patriotism on the part of an American wishing to help his government, it somehow became, at least in some people's eyes, something terrible.

We have had movies – *The Day of the Condor* – others that have portrayed the CIA as a rogue agency, out of control, and the most patriotic thing that an American can do is to frustrate it, denounce it, expose it.

And that's why you have the kinds of problems that you have.

If we could get back to the point, Mr. Chairman, where Americans feel that protecting their country is a logical thing for them to do, and cooperating with their country's legitimate intelligence activities is a logical thing for them to do, you can once again have major national publications give business cards out to people who travel, travel as reporters, can come back with information that can be part of the activity.

If there are high-level defections of the kind we've seen represented at the table here today, they can be facilitated. And you do not have the situation you've described where the flag is planted and everybody knows where to shoot, metaphorically, of course.

Mr. Fairchild. I agree 100 percent, Senator.

Senator Bennett. I think we all have an obligation to change the culture among Americans who travel abroad or who do business abroad to get back to the days when we say, it is an American's patriotic responsibility to assist in trying to stop the intelligence leak or provide assets with which it can be dealt with.

Representative Saxton. Thank you, Senator.

Mr. Eftimiades, let me ask you about Hong Kong and China and the relationship, and whether or not we should be concerned about export of what today is termed dual-use technologies.

And let me frame the question this way.

A week or so ago, I was approached by some folks that were concerned about the pending or potential export of some dual-use technology to China. I felt rather outraged that a, frankly, weapons system that I helped create here was being commercialized, which was fine, to commercialize it. But that the commercialized version would be sold to China.

And so I raised the question in appropriate circles here.

A few days later, I saw a small article in one of the U.S. defense publications that there was no intent on the part of the contractor to do any such thing with regard to China.

At which point an employee of the company called me and said, you should have asked them the question in the context of Hong Kong.

Now, we have different American export laws. A set of export laws for China and a set of export laws for Hong Kong.

The case is being made here by some that because there is a one-China-Hong Kong political entity, but a two-China-Hong Kong commercial trade entity, that people like me don't have to worry about these issues.

Now I find that, given what I have heard here and before today, I find that hard to believe.

Mr. Eftimiades. Sir, to comment on that, I wrote in my book what my findings were. After looking at over 10 years of significant export and enforcement cases by U.S. Department of Justice and the Department of Commerce denial orders from '86 up through '93.

It was clear in that case that the most frequent operational pattern of Chinese intel to acquire U.S. technology was through cover and front companies in Hong Kong, making connections to the United States and using Hong Kong as a transit place.

In fact, I took the Department of Commerce denial orders and took all the listings of companies listed there for those eight or nine years or so, and dumped them into my computer. I went back and got the Hong Kong phone books for that time period and did a cross-check from my computer and had numbers and numbers and numbers of cases where a Hong Kong company was put on the sanctions list by the Department of Commerce, only to occur with a different company name, same address, same telephone number two years later in Hong Kong.

They put a new shingle on the door, turned around and did it again.

Total cost of business – $35,000 fine for them. Not a problem. It's a dramatic problem.

Hong Kong has been – I don't know how – and to be frank with you, I haven't looked and seen if we have a change of law that's come into being because of Hong Kong becoming part of the People's Republic of China.

But as far as the operational pattern is concerned, it's done through Hong Kong. That is the primary way.

Representative Saxton. Thank you. Would you and/or Mr. Fairchild care to comment on the situation involving India and the nuclear tests that recently occurred there, as well as Pakistan and anything that you might have to add to the national conversation that's ongoing about that, keeping in mind that we're going to have to close up shop here in about five minutes because those bells that we've been listening for finally rang.

Mr. Eftimiades. Well, in that case, I'll take the opportunity to defer to Mr. Fairchild.

Mr. Fairchild. I was going to defer to you.

(Laughter)

No, actually, Mr. Chairman, I'm sorry. I don't have any specific information or knowledge of that area. However, in my written statement, I used India as an example of what many people consider to be an intelligence failure.

If an intelligence agency can't tell you the date and time that a specific event is going to take place, that's considered a terrible intelligence failure. And I tried to make the point that an intelligence agency, by virtue of the fact of its existence, cannot answer every specific question that's put to it.

And more to the point, the question would be, how much information over a period of time has the DO provided to policy-makers? Did they provide enough information which would make the policy-makers have a reasonable understanding and a reasonable expectation that these tests would take place?

So, in that frame, that's how I used the example of India. But as far as the nuclear test is concerned, I have no specific knowledge.

Representative Saxton. Well, I would like to thank each of you for being here today – Mr. Sheymov, Mr. Alibek, Mr. Eftimiades, and Mr. Fairchild.

Thank you very much for your contribution. I wish we could stay longer. Unfortunately, things don't stand still on Capitol Hill, as you know.

I hope we'll be able to call on you in the future as the dialogue that we're involved in on these subjects takes place and goes forward.

Thank you very much for being here today. We appreciate it.

Mr. Alibek. Thank you.

Mr. Fairchild. Thank you, Mr. Chairman.

Mr. Eftimiades. Thank you, sir.

Mr. Sheymov. Thank you.

[Whereupon, at 11:45 a.m., the hearing was concluded.]

SUBMISSIONS FOR THE RECORD

PREPARED STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

I am pleased to welcome our distinguished panelists before the Joint Economic Committee (JEC) this morning.

As we reach the end of this century and enter the next one, we must anticipate and prepare for the changes, new realities, and challenges that will come in the near future. How we handle those challenges will determine our success in the millennium ahead. Unpreparedness and the exercise of bad judgement could put the United States in a significantly disadvantaged position economically and militarily, and it could even threaten our national security.

It is the opinion of many experts, a few of whom will testify today, that terrorists and the intelligence services that support terrorists will step up attacks using electromagnetic pulse weapons and biological weapons. Terrorists will continue to deny responsibility while maintaining the capabilities to continue the high-profile attacks.

Many believe, as do I, that our success in High Technology Warfare has deterred our enemies and, in many ways, contributed to the conclusion of the Cold War. Our continued success in the Gulf War made it very clear that to challenge the United States conventionally was a death sentence.

It is this very success in conventional warfare that has caused those who hate democracy, the West, and everything the United States stands for, to create new weapons heretofore unknown or unmentioned. While these new weapons are being developed, our enemies increasingly strengthen their commitment in terms of manpower, money, and intelligence services capabilities, particularly in the areas of covert actions, counter intelligence, and surveillance.

That, I would suggest, could have significant national security and economic impact on the United States. We need to develop our defensive and offensive capabilities against the new and improved weapons of mass destruction and demand that our intelligence services develop a new and dynamic pursuit of counter intelligence and operational security capability for the millennium.

We, the Congress, must be prepared to eliminate our obsolete Cold War institutions and create new and dynamic organizations quickly

because we simply do not have time to waste in maintaining a status quo that is irrelevant to the preservation of the nation into the next century.

I will now introduce our witnesses for today's hearing:

Before we begin, I want to thank each of you for your hard work, dedication, and commitment, which has oftentimes required great personal risk. The United States is a better nation, and its citizens are much safer because of your courage and dedication.

Our first witness is Mr. Victor Sheymov, who defected to the United States from the Soviet Union in 1980. At that time, he was a Major in the 8th Directorate of the KGB – the Russian equivalent of our National Security Agency. His last position in the KGB involved the coordination and responsibility for the overall security of the KGB's foreign cipher communications. Mr. Sheymov graduated from Moscow State Technological University, and was a researcher at the Russian Military Research Institute. He has also worked within the Soviet "Star Wars" program and has written a book, entitled *Tower of Secrets*.

Our second witness, Dr. Kenneth Alibek, defected to the United States in 1992. At that time, Dr. Alibek was the First Deputy of the Soviet Union's Offensive Biological Warfare Program and a retired Colonel of the Soviet Army. Dr. Alibek holds a medical degree in infectious diseases, a Ph.D. in microbiology, and a Doctor of Science in industrial biotechnology.

Dr. Alibek spent 21 years in pathogen laboratories studying the production of many types of biological weapons, such as plagues and anthrax. He also developed medical protocols for the treatment of these diseases, and for the treatment of mass casualties caused by biological weapons. Since his arrival in the United States, Dr. Alibek has worked with various government agencies and is currently continuing his work combating biological weapons.

Our third witness is Mr. Nicholas Eftimiades, who currently works for the Defense Intelligence Agency (DIA). He is here today as the author of his book, *Chinese Intelligence Operations,* which is considered to be the first ever scholarly analysis on the subject and has been translated into four languages. He has also held positions in the Central Intelligence Agency (CIA), with the counter-intelligence staff at the State Department, and has been a naval officer.

Mr. Eftimiades has written numerous articles and a monograph entitled "China's Ministry of State Security: Coming of Age in the International Arena." For this work, he was awarded the "Scholarly Work of the Year on Intelligence" by the National Intelligence Center.

He is also the recipient of the Director's Intelligence Medal by the Defense Intelligence Agency.

Mr. Eftimiades graduated from George Washington University with a B.A. in East Asian studies and a Master's in strategic intelligence from the Joint Military Intelligence College.

Our final witness is Mr. Brian Fairchild. From September 1976 to October of 1995, Mr. Fairchild was a staff operations officer in the Directorate of Operations of the Central Intelligence Agency. Mr. Fairchild is also a former member of the Army's elite special force – the Green Beret. He is a graduate of California State University with degrees in international relations and Asian studies, and speaks several Asian and European languages. Mr. Fairchild is now retired from the CIA and owns his own company.

Well, ladies and gentlemen, if you are not impressed, you should be!

PREPARED STATEMENT OF VICTOR SHEYMOV, COMSHIELD CORPORATION

The Low Energy Radio Frequency Weapons Threat to Critical Infrastructure.

Mr. Chairman, members of the Committee,

I thank you for your concern and attention to the problem of terrorism, to the potential exploit of latest technological achievements of this country by terrorists and other criminal groups. I also would like to thank you for this opportunity to bring attention to a potentially dangerous and costly impact of the possible use of radio frequency (RF) weapons by terrorists and criminals. Special uses of RF technology were a major part of my 27 years of involvement in intelligence, security, and technology matters, and I would like to share my knowledge and experience into this are which is often misunderstood and largely ignored. I have somewhat split responsibility in this open hearing: I want to shed some light on the problem but, at the same time, to avoid revealing crucial information to the terrorists who undoubtedly are tuned in.

Within the wide ranging means of Information Warfare (IW), one of the prominent places belongs to IW attacks on computers and computer-based equipment. Leaving physical destruction of computers aside, the IW attacks on computers could be classified as attacks through legitimate gateways of the computer such as the modem and the keyboard (software attacks), and attacks through other than legitimate gateways (backdoor attacks). At the current technological level, backdoor attacks can be carried out mainly by utilizing radio frequency (RF) technology and thus can be classified as RF attacks.

Vulnerability of computers to software attacks is widely recognized, and efforts with substantial funding are underway with the goal of developing protective technology to neutralize such attacks. The backdoor attacks, on the other hand, have little official recognition, and adequate efforts to develop adequate protective technology do not seem to have taken place.

One premise underlies many special applications of RF technology and is based on a principal that any wire or electronic component is, in fact, an unintended antenna, both transmitting and receiving. Importantly, every such unintended antenna is particularly responsive to its specific resonance frequency, and to some extent, to several related frequencies. It is not responsive to all other frequencies under normal conditions. If

an objective is to eavesdrop on the device, then the EM emanations coming from functioning components of the device are received by highly sensitive receiving equipment and processed in order to duplicate information handled by the device. If an objective is to influence the device's functioning, then appropriate RF signals are transmitted to the targeted device. That RF signal, being received by pertinent components of the device, would generate a corresponding signal within the device. Producing and transmitting a signal which would effectively control the targeted device through a "back door" attack is an extremely difficult task that requires technology and expertise available only in two or three countries is the world. At the same time, producing and transmitting a signal which would just disrupt the normal functioning of the target devise is a much simpler technological task. It can be classified as a jamming "back door" attack, or jamming RF attack. Conceivably, it can be done by a large number of parties.

Jamming RF attacks can utilize either high energy radio frequency (HERF), or low energy radio frequency (LERF) technology. HERF is advanced technology, practical applications of which are still being developed. It is based on concentrating large amounts of RF EM energy in within a small space, narrow frequency range and a very short period of time. The result of such concentration is an overpowering RF EM impulse capable of causing substantial damage to electronic components. The HERF impulse is strong enough to damage electronics components irrespective of their specific resonance frequencies.

LERF technology utilizes relatively low energy, which is spread over a wide frequency spectrum. It can, however, be no less effective in disrupting normal functioning of computers as the HERF due to high probability that its wide spectrum contains frequencies matching resonance frequencies of critical components. Generally, the LERF approach does not require time compression, nor does it utilize high-tech components. This technology is not new and well known, albeit to limited circles of experts in some exotic subjects, such as Tempest protection. LERF impact on computers and computer networks could be devastating. One of the dangerous aspects of a LERF attack on a computer is that an unprotected computer would go into a "random output mode." This simply means that it is impossible to predict what the computer would do. The malfunction could differ from a single easily correctable processing error to a total loss of its memory and operating system, to giving a destructive command given to controlled by computer equipment. Furthermore, differently from a simple computer failure, any

level of redundancy cannot solve the problem. This point is rarely realized by computer users with the assumption that a back-up computer provides a comfortable level of safety. This is certainly not true in regard to a LERF attack.

U.S. military puts high priority on minimizing collateral damage and applies high requirements to its weapons systems' accuracy. HERF weapons' accuracy is relatively high, but it is not yet quite up to the military requirements. But this certainly is not a deterrence for terrorists because collateral damage is what they are usually after in the first place. Considering known utilization of latest technology by terrorists and drug cartels around the world, it is likely that HERF technology can be obtained and used by these criminal enterprises in near time, possibly even before it finds its wide acceptance within the military.

Differently from HERF, LERF weapons are notoriously inaccurate, virtually by definition. LERF weapons' impact on computers is devastating and highly indiscriminate. A very high percentage of computers within an effective range of a utilized LERF weapon will malfunction. This is very likely to make these weapons an attractive choice for terrorists. While HERF weapons were substantially covered during this Committee hearing on this subject in February of 1998, some details of LERF weapons seem to be worth discussing.

Contrary to a popular belief, different kinds of LERF weapons have already been used over the years, primarily in Eastern Europe. For instance, during the Czechoslovakian invasion in 1968, the Soviet military received advanced notice that Czechoslovakian anti-Communist activists had been wary of relying on the telephone communications controlled by the government, and prepared to use radio transceivers to communicate between their groups for coordination of their resistance efforts. During the invasion Soviet military utilized RF jamming aircraft from the Soviet air force base in Stryi, Western Ukraine. The aircraft were flying over Czechoslovakia, jamming all the radio spectrum, with the exception of a few narrow pre-determined "windows" of RF spectrum utilized by the invading Soviet army. This measure was successful, effectively nullifying communications between the Czechoslovakian resistance groups.

Another example of a LERF attack was the KGB's manipulation of the United States Embassy security system in Moscow in the mid-80s. This was done in the course of the KGB operation against the Embassy which targeted the U.S. Marines there. The security system alarm was repeatedly falsely triggered by the KGB's induced RF interference

several times during the night. This was an attempt to annoy and fatigue the marines and to cause the turning of the "malfunctioning" system off.

Additional example of an RF attack was when the KGB used it to induce fire in one of the equipment rooms in the U.S. Embassy in Moscow in 1977. A malfunction was forced on a piece of equipment. It caught fire, which spread over a sensitive area of the Embassy. The KGB tried to infiltrate its bugging technicians into the sensitive area under the cover of the firefighters who arrived immediately after the fire started. A similar event occurred at the British embassy in Moscow several years earlier.

These examples illustrate a much more advanced use of RF technology than a simple disruption of computers in a radius of several hundred yards from the unleashed "RF bomb". An example of such a device was designed and built by the KGB in late 70-s. The device was built for completely different purpose and was not used to disrupt computers. However, its potential as an "ARF bomb" was clearly realized at the time. Its reference cost was within one hundred dollars, size of about a shoe box, and it could be easily assembled within two-three hours with general purpose tools and components readily available in an average electrical store. The only obstacle on the way of this technology to terrorists' arsenals is a know-how, fortunately limited to a small number of experts in a few countries. However, some of these experts are experiencing very difficult economic conditions in Russia. On the other hand, a sizable cash offer tempting to these experts could come from any of the well funded terrorist groups at any time. This situation seems to indicate that relying on these two potentially explosive components remaining separate from each other is less than wise.

Being a technological leader of the world, the United States has been vulnerable to an RF attack more than any other country for some time. This vulnerability significantly increased during last fifteen years with wide utilization of computers in every aspect of this country's functioning. At this time it is very difficult to find an area which would not rely heavily on computers. In fact, this country is so dependent on computers that many even vital functions cannot be performed manually. At the same time, it is important to realize that all those computers performing important and vital services are not protected from an RF attack. Areas like air traffic control, commercial airliners, energy and water distribution systems, and disaster and emergency response services represent attractive targets for terrorists. At the same time these systems are totally open to an RF attack. By the nature of computers and

computer networks, the failure of one sub-system would trigger a snow-balling effect with second, third, and following chain failures. The full effect of such an event is difficult even to predict, lest to neutralize, unless computers and computer networks are reliably protected against RF weapons. A serious RF attack on critical infrastructure would have an impact of national level with numerous losses of life and incalculable economic damage. Besides the show-balling effect of computer failures, there could be a crippling effect if RF weapons used in concert with any other type of terrorist attack. Most of the responses to other forms of terrorist attacks are designed with the assumption that the computers of the response service are working and such functions as traffic control are intact. With an additional RF attack, concerted with the primary one, this assumption is not valid. Communications and transportation of the response teams could be crippled with a tragic impact on rescue efforts.

Even a single limited and attack could have serious consequences. For instance, an attack on computers of financial markets could have a world-wide implications with losses easily reaching multi-billion levels.

In addition to intentional RF interference, current technological developments lead to a problem of unintentional RF interference. Indeed, with the speed of modern computers and their miniaturization advancing at a rapid pace, their working frequency and sensitivity to RF emanations is also increasing. This leads to unavoidable interference conflicts, some of which have already shown themselves and led to an intermediary solution of regulatory nature. For instance, even barely emanating electronic equipment such as lap-top computers and electronic games needs to be turned off during take-off and landing of commercial airliners.

Another aspect of offensive RF technology is its traditional application in information intercept or eavesdropping. Traditionally, the Soviet Union and Russia have placed high priority on the development and use of this technology. Being one of the two "superpowers" in this area, Russia considers its spending on RF offensive operations a very wise and profitable investment.

Changes of last decade in Russia impacted the KGB, which has been split into independent parts. The 8th and 16th Directorates, roughly representing Russian equivalent of the NSA, became an independent agency, the Federal Agency of Government Communications and Information (FAPSI, as a Russian acronym). FAPSI is directly subordinate to the President of Russia. In a wave of privatization, FAPSI was partially "privatized" as well. Some of the leading FAPSI experts

left the agency and founded private security companies, taking best officers of all levels along. These companies cater mainly to Russian private financial institutions and provide a wide range of security services. They are fully capable of carrying out any defensive and offensive operations with equal level of confidence.

The concentration of world-class experts on offensive electronic operations in these few companies by far surpasses any private entity in the world and exceeds capability of most governments. These experts can easily intercept and provide to their clients virtually any commercial information of any country. Commercially available means of electronic information security present no practical difficulties for them. Intercept of commercial and financial information could be extremely profitable and create the capability to manipulate international financial markets as well as to carry large scale international money-laundering operations with very limited operational risk.

Financial success of these FAPSI private spin-off companies and high earnings of their employees make them very attractive "golden parachutes" for the remaining FAPSI officers. Combined with traditionally close ties, this leads to continuing effective technological and personnel cooperation between the FAPSI and these companies. At the same time, the end of the Cold War somewhat shifted goals, objectives, and some targets of the FAPSI toward a heavier emphasis on intercept of technological, commercial and financial information. In this regard, some of the targets are easier to attack from a position of a private company. This leads to a likely close operational cooperation between the FAPSI and its private spin-off companies. The private companies can provide the FAPSI with some of the products of their intercept, while FAPSI can also share some of its products, along with personnel and equipment, including its powerful and sophisticated facilities, such as the Lourdes in Cuba, for a very productive long-range intercept.

This situation can easily put American private business in a highly unfavorable competitive position.

All of the above seems to demonstrate an urgent necessity to develop technology for computer protection against both intentional and unintentional RF interference, as well as against illegal intercept of sensitive and proprietary information by foreign competitors. It can take a few days to build a LERF weapon. It takes a few weeks or a few months to establish a successful collection of information through RF intercept. However, it should be realized that developing adequate computer protective technology, even for limited applications, would

take at least two years. There seems to be a certain disconnect between appropriate U.S. technical experts and political decision makers, who are ultimately responsible for strategic course of technological efforts of this country. This disconnect needs to be mended and coordinated efforts should take place for developing protection of computers against RF attacks.

In conclusion, I would like to state that it seems that the question that we are facing is not whether we need to develop adequate RF protective technology or whether we can afford to protect our computers from possible RF attacks. The real question is whether we can afford to not protect at least critical infrastructure computers. The ultimate decision on this dilemma is a prerogative of the United States Congress.

I would like to thank you again for your kind invitation to appear before this Committee and for this opportunity to comment on a very important matter.

PREPARED STATEMENT OF KENNETH ALIBEK
PROGRAM MANAGER, BATTELLE MEMORIAL INSTITUTE

Mr. Chairman and members of the Committee, thank you for the opportunity to discuss the issues of biological weapons and biological terrorism with you. I am in a rather unique position to discuss these issues, since I developed biological weapons for the Soviet Union for nearly twenty years, until my defection in 1992. When I left the Russian biological warfare program, I had been serving for four years as First Deputy Director of Biopreparat. Biopreparat, the civilian arm of the biological weapons program, comprised over half of the entire program's personnel and facilities. At that time, I was responsible for approximately 32,000 employees and 40 facilities. Since arriving to the United States, my personal and professional goal has been to make the greatest contribution I can to eliminating the danger of biological weapons.

What are biological weapons?

Biological weapons are weapons of mass destruction (or mass casualty weapons, to be precise, since they do not damage nonliving entities) that are based on bacteria, viruses, rickettsia, fungi, or toxins produced by these organisms. Compared to other types of weapons (nuclear, chemical or conventional), biological weapons are unique in their diversity. Dozens of different agents can be used to make a biological weapon, and each agent will produce a markedly different effect. These differences in effect are shaped by various properties of the particular agent, such as its contagiousness, the length of time after release that it survives in the environment, the dose required to infect a victim, and of course the type of disease that the agent produces.

Although most people think of biological weapons as anti-personnel weapons, some biological weapons are designed to destroy crops or livestock. In the future, it is theoretically possible that new types of biological weapons will be produced that:

damage military equipment by causing corrosion degrade different types of plastics used in equipment, computers, etc. render fuels useless.

Biological weapons formulations are of two types: a liquid or a dry powder. For most agents, the liquid form is easier to produce, but the dry form stores longer and disperses better when deployed. The basic steps for creating a liquid biological weapon are:

obtaining a sample of the microorganisms to be used

culturing the microorganisms until there is enough for a weapon

concentrating the culture to make it strong enough for a weapon

adding certain ingredients to stabilize the culture.

For a dry weapon formulation, this liquid culture is dried out and then ground up into microscopic particles. For toxin weapons, the toxin must first be extracted from the source-either the liquid bacterial culture or a plant or animal-and then concentrated.

Biological weapons are relatively inexpensive and easy to produce. Although the most sophisticated and effective versions require considerable equipment and scientific expertise, primitive versions can be produced in a small area with minimal equipment by someone with limited training.

Biological weapons can be deployed in three ways:

contamination of food or water supplies, which are then ingested by the victims

release of infected vectors, such as mosquitoes or fleas, which then bite the victims

creation of an aerosol cloud, which is then inhaled by the victims (or, if the targets are plants, the cloud then settles on and infects the plants).

Since the U.S. has highly effective water purification systems, contamination of the water supply is the least effective method for disseminating a biological weapon in this country. Contamination of food supplies would most likely be used in a terrorist rather than a military attack, since it is difficult to contaminate enough food to gain a military advantage. Release of infected vectors is not particularly efficient for either military or terrorist purposes and entails a high probability of affecting those producing the weapons or living nearby.

By far, the most efficient and effective mode for applying biological weapons is creation of an aerosol cloud. Such a cloud is made up of microscopic particles and is therefore invisible. It can be produced in several ways, all of which involve either an explosion (a bomb or a bomb within a missile) or spraying (usually involving a special nozzle on a spray tank). The effectiveness of the cloud is determined by numerous factors, such as the amount of agent that survives the explosion or spraying, and the wind and weather conditions. The primary result of an effective cloud is simultaneous infections among all those who were exposed to a sufficiently dense portion of the cloud. In addition, agents that can survive for a long time in the environment will eventually settle, contaminating the ground, buildings, water and food sources, and so on.

In some cases, these sediments can form another dangerous aerosol cloud if they are disturbed.

The USSR'S biological weapons program

Although the Soviet Union was a party to the 1972 Biological and Toxin Weapons Convention, it continued a high-intensity program to develop and produce biological weapons through at least the early 1990s. The size and scope of this program were enormous. For example, in the late 1980s and early 1990s, over 60,000 people were involved in the research, development, and production of biological weapons. Hundreds of tons of anthrax weapon formulation were stockpiled, along with dozens of tons of smallpox and plague. The total production capacity of all of the facilities involved was many hundreds of tons of various agents annually.

The Soviet Union's biological weapons program was established in the late 1920s. Prior to World War II, research was conducted on a wide variety of agents. By the beginning of the war, the Soviet Union was able to manufacture weapons using the agents for tularemia, epidemic typhus, and Q fever, and was also working on techniques for producing weapons using the agents for smallpox, plague, and anthrax. My own analysis of a tularemia outbreak among German troops in southern Russia in 1942 indicates that this incident was very likely the result of the USSR's use of biological weapons. There was also a suspicious outbreak of Q fever in 1943 among German troops vacationing in the Crimea.

World War II brought several advances for the Soviet biological weapons program. First, the USSR gained access to German industrial techniques and machinery for manufacturing large-scale biological reactors and other industrial equipment. Second, the Soviets obtained valuable information from the Japanese biological weapons program. This information gave the Soviet program an instant boost in its development.

After the war, the Soviet program continued to expand and develop. In many cases, it closely shadowed the U.S. biological weapons program. While the pre-war list of weaponized agents included tularemia, epidemic typhus, and Q fever, the post-war list was expanded to include:

smallpox

plague

anthrax

Venezuelan equine encephalomyelitis

Glanders

brucellosis

Marburg infection.

Numerous other agents were studied for possible use as biological weapons, including:

Ebola

Junin virus (Argentinian hemorrhagic fever)

Machupo virus (Bolivian hemorrhagic fever)

yellow fever

Lassa fever

Japanese encephalitis

Russian spring-summer encephalitis.

Techniques and equipment were developed and refined for more efficient cultivation and concentration of the agents. Methods for producing dry weapons formulations for a number of agents were also developed. In addition to weapons to affect humans, a number of weapons to affect crops and livestock were developed using such agents as:

psittacosis (affects fowl)

ornithosis (affects fowl)

Rinderpest virus (affects cattle)

African swine fever virus (affects swine)

wheat stem rust spores (affect wheat crops)

rice blast spores (affect rice crops).

During this post-war period, which lasted until the signing of the 1972 Biological and Toxin Weapons Convention, the Soviet Union also formulated its doctrine regarding the production and use of biological weapons. In the Soviets' definition, "strategic" weapons were those to be used on the deepest targets, i.e. the U.S. and other distant countries; "operational" weapons were those intended for use on medium-range targets, nearer than the strategic targets but well behind the battlefront; and "tactical" weapons were those to be used at the battlefront. Biological weapons were excluded from use as "tactical" weapons, and were divided into "strategic" and "operational" types. "Strategic" biological agents were mostly lethal, such as smallpox, anthrax, and plague; "operational" agents were mostly incapacitating, such as tularemia, glanders, and Venezuelan equine encephalomyelitis. For both types of weapons, use was envisioned on a massive scale, to cause

extensive disruption of vital civilian and military activity. The Soviets also established so-called mobilization capacities: facilities whose peacetime work was not biological weapons production, but which could rapidly begin weapons production if war was imminent.

It is important to note that, in the Soviets' view, the best biological agents were those for which there was no prevention and no cure. For those agents for which vaccines or treatment existed-such as plague, which can be treated with antibiotics-antibiotic-resistant or immuno-suppressive variants were to be developed. This is in sharp contrast to the philosophy of the U.S. program (terminated in 1969 by President Nixon's Executive Order), which stringently protected the safety of its biological weapons researchers by insisting that a vaccine or treatment be available for any agent studied.

After the Soviet Union became a party to the 1972 Biological and Toxin Weapons Convention, internal debate ensued about the fate of the existing biological weapons program. The end result was that the program was not dismantled, but further intensified. During the period 1972-1992, the focus of the program was expanded. In addition to continuing previous types of work (developing improved manufacturing and testing techniques and equipment; developing improved delivery means for existing weapons; and exploring other possible agents as weapons), new emphasis was placed on:

- conducting molecular biology and genetic engineering research in order to develop antibiotic-resistant and immunosuppressive strains and to create genetically combined strains of two or more viruses
- studying peptides with psychogenic or neurogenic effects as possible weapons
- transforming non-pathogenic microorganisms and commensals into pathogenic microorganisms
- testing all of the facilities considered part of the "mobilization capacity" to verify their readiness.

During this period, the Soviet program not only caught up with the U.S. program (which was halted in 1969), behind which it had lagged by about five years, but it became the most sophisticated biological weapons program in the world by far.

However, as the Soviet Union weakened during the late 1980s and early 1990s, and as more and more detail was revealed regarding the Soviet biological weapons program, the West put increasing pressure on

the Soviets. In 1991, a series of trilateral inspections were conducted among the United States, Great Britain, and the Soviet Union. Note that the Soviet program still existed when these inspections took place; the Soviets covered up the evidence as best they could.

After the collapse of the Soviet Union, in early 1992, Russian President Boris Yeltsin signed a decree banning all biological weapons-related activity. Considerable downsizing in this area did indeed occur, and included destruction of existing biological weapons stockpiles. However, there still remains doubt that Russia has completely dismantled the old Soviet program.

Why am I concerned about biological weapons in Russia today?

Certainly, now that the Cold War is over and U.S.-Russia relations have changed markedly for the better, Russia presents far less of a military threat to the U.S. However, it would not be prudent to consider that Russia presents no military threat whatsoever. In addition, biological weapons technology can possibly proliferate from Russia to other countries less friendly to the U.S. For these reasons, it is important that we continue to analyze the situation with biological weapons in Russia.

There are three main reasons that I am concerned about possible biological weapons research and development in Russia today. First, many of Russia's former biological weapons facilities have never been subjected to international inspections. Second, Russia continues to publicly deny the size or even existence of many aspects of the former Soviet program. And third, among Russian scientists' published work, there are many studies I feel are dual-purpose or even outright offensive biological weapons work.

The Russians have steadfastly refused to open their military biological weapons facilities to international inspection. Pursuant to agreements between Russia, the U.S. and Britain, a series of trilateral inspections was begun in 1991. However, the facilities visited in Russia were those managed by the civilian arm of the Soviet/Russian biological weapons program, Biopreparat. The facilities of the Ministry of Defense, most notably those at Sergiyev Posad (formerly Zagorsk), Kirov, Yekaterinburg, and Strizhi, have never been inspected. Furthermore, according to the On-Site Inspection Agency, the last visits to Russian civilian facilities took place in early 1994.

Russia continues to deny various aspects of its former biological weapons program. The 1996 Annual Report of the U.S. Arms Control

and Disarmament Agency states that, "The Russian Federation's 1993-1996 BWC data declarations contained no new information and its 1992 declaration was incomplete and misleading in certain areas." Note that 1992 is the year that the Russians supposedly "came clean" by acknowledging and then dismantling their offensive biological weapons program. Until the Russians have provided a complete accounting of their past biological weapons activities, however, it is difficult to believe that they have ceased all of these activities.

In this regard, certain people in the Russian government even seem to be backpedaling, denying incidents previously acknowledged and returning to Cold War rhetoric. Consider the following excerpts from an interview with Lieutenant General Valentin Yevstigneyev, the head of the 15th Directorate of the Russian Ministry of Defense until 1992. At that time, this directorate was the military arm of Russia's biological weapons program. He is now the Deputy Director of the Ministry of Defense's NBC Defense Directorate.

The interview was published in the Russian newspaper Izvestiya on March 3, 1998; the full translated text of the article is attached. The interviewer is questioning Yevstigneyev about the 1979 anthrax incident in Sverdlovsk (now Yekaterinburg), which is now widely known to have been the result of an accidental release of anthrax spores from a military production facility there. At that time, the Sverdlovsk facility was producing and stockpiling scores of tons of anthrax biological weapon formulation annually.

> **Interviewer**: Do you claim, as before, that in 1979 on the Sverdlovsk-19 military base, no explosions of munitions with a "biological" filling nor massive deaths occurred?
>
> **Yevstigneyev**: People who don't know much about bacteriology might be able to believe the newspaper stories (which, by the way, is indeed happening now). The professionals simply laugh.
>
> International experts found four different strains (of the virus culture-author's note) of anthrax. Four different bacteria! Different, you understand? If a bomb exploded, would there really be four strains? How can you explain that people fell ill 50 kilometers away, but on the military base, where this explosion supposedly occurred, no one fell ill? Next door to the base is a tank division-two fatal cases...

Believe me, if this was a single military release, two or three days and everyone would be finished!

Meanwhile, no one writes that several carcasses of cows with anthrax were brought into the brick factory to be burned in the furnace. But anthrax does not burn in a fire! The spores could have been carried off to anywhere through the chimney. The spores themselves live hundreds of years. As an example, no one has been able to live on the English island of Gruinard since the second world war. Biological weapons were tested there, including anthrax...

I was not yet at Sverdlovsk-19 in 1979. But in 1985 I was appointed the deputy director of the institute for scientific work. Of course, I tried to analyze the situation. I did a computer analysis using image recognition theory and mathematical modeling, and I tried three versions: the institute was responsible, a natural epidemic, and a diversion with the aim of compromising the institute. Strangely enough, the latter version got the highest score.

Interviewer: In the documentary film, "The Generals and Anthrax," a worker speaks on camera about the existence of a section for manufacturing biological munitions. The Ministry of Defense regards this film as truthful. Does this mean that there was an underground factory after all?

Yevstigneyev: There was a shop where we really did make 4 samples of the American one-pound, two-pound and four-pound bombs. The worker, literally on his knees, made these "toys." But there was no other way-we had to learn how to evaluate the biological situation, if such weapons would be used. We assembled munitions, went out to an island in the Aral Sea, set up biological reconnaissance equipment, observed what kind of cloud formed, and so on... Now we have magnificent calculations which everyone is using, beginning with the Ministry of Defense itself and ending with the Ministry for Emergency Management.

But this was done considerably before the epidemic. In 1979, in a refrigerator of the laboratory of Sverdlovsk-19, only a few ampoules of anthrax bacteria were stored for vaccine testing. All of the powers that be knew this, which is incidentally why they pointed the finger at us.

In fact, Yevstigneyev goes so far as to resurrect the Cold War-era accusation that the AIDS virus was created intentionally by a foreign nation, and implies that the U.S. is the likely culprit:

> Yevstigneyev: There are serious suspicions that AIDS was created in a military laboratory abroad. Several black volunteers from prison were infected, but the analysis gave a negative result. They still didn't know that the incubation period could last for decades... The volunteers were released, and the situation got out of control. There are some African countries in which up to 80% of the people are HIV-infected.

Other references have appeared in the Russian press about the non-destruction, or even re-creation, of offensive biological capacities. Obviously, I am not able to substantiate these claims, and the articles appearing in the Russian press are certainly not without their inaccuracies. However, when I compare the details reported on the Soviet program prior to 1992 with my own knowledge, I find that the journalists have amassed a surprising amount of accurate information. Therefore, I am inclined to give their assertions serious consideration. For example, here are two excerpts from the 1998 No. 4 issue of *Top Secret*, a Russian monthly newspaper:

> The editorial board [of this paper] specifically knows that the archives of [the facilities at] Kirov and Sverdlovsk-19 are completely preserved. We also have the indications of a former highly placed employee of The [Biological Weapons] System, who confirms that as late as 1995 all of the archives of P.O. Box A-1063 [another code name for the biological weapons system] were systematized and prepared for long-term storage...

The same newspaper gives a quote from an interview of Major-General Khorechko in the anniversary edition of the Sverdlovsk-19 base newsletter:

> Now we are in effect building the factory which was destroyed in 1986-89 [the years in which much of the facility's anthrax production capability was dismantled in response to severe pressure from the West and impending site inspections].

The published scientific literature coming out of Russia contains research of a dubious nature. Granted, each of the published works I have seen can be justified in some way-as research in biological defense, as vaccine studies, and so on. And I am not able to state with 100%

certainty the intent of the Russian government in conducting this research. However, based on my knowledge of the priorities and deception tactics of the Soviet/Russian program as of late 1991, the current research in many cases appears to be continuing in the same vein. I will provide examples using work on a single agent, the smallpox virus.

Possession of the smallpox virus was limited by World Health Organization mandate to two facilities, the CDC in Atlanta and the Ivanovsky Institute for Viral Preparations in Moscow. However, in the late 1980s, I oversaw the development of the USSR's tactics to circumvent both this restriction and the 1972 Biological and Toxin Weapons Convention. In very general terms, our research and concealment plans were as follows:

Do everything in our power to have the USSR's repository for smallpox virus transferred from the Ivanovsky Institute, which was not involved in any biological weapons research, to the State Center for Virology and Biotechnology "Vektor" in Koltsovo, near Novosibirsk. In the late 1980s, "Vektor" was doing biological weapons research on smallpox virus; the repository transfer would provide a plausible "cover story."

Explore the genome of the smallpox virus as fully as possible, to facilitate genetic engineering operations with it and to enable an accurate comparison with related viruses. This research work was easily justified, as it also had a legitimate purpose. Since the WHO was planning to destroy the last remaining stores of smallpox virus, it was important to completely sequence the smallpox genome for future studies.

Using this genetic analysis, identify viruses closely related to smallpox that could be substituted for smallpox virus in the bulk of the experiments. The viruses used most often were vaccinia (used for smallpox vaccination), ectromelia (mousepox), and monkeypox.

Perform genetic engineering work on these viruses, with the eventual aims of manipulating smallpox virulence factors and inserting genes of other viruses into smallpox to create chimera viruses. (The point of creating chimera viruses was to design new organisms that would have a synergistic effect and/or evade current vaccines or treatments.) A chimera strain involving insertion of Venezuelan equine encephalomyelitis (VEE) genes into smallpox was created in the late 1980s. Using the technique described above of substituting related viruses for smallpox, a

chimera strain of ectromelia and VEE was created for initial testing.

Claim that the genetic engineering work we were doing was for the purposes of developing new vaccines, especially for research using vaccinia virus. (I was skeptical that this argument would be convincing to the international community. Vaccinia is not the ideal vector for a vaccine because of the adverse reactions it can elicit and because many other possible vectors exist.)

Here is what I am now seeing in the published literature, which in my opinion constitutes a continuation under the above-noted plans:

The official repository for the smallpox virus was transferred from the Ivanovsky Institute to "Vektor" in 1994. (My understanding of this transfer is that the Russian government presented it to the World Health Organization as a fait accompli in 1994.)

The genome of smallpox virus has been fully analyzed and compared to the genome of vaccinia.

Extensive genetic engineering research has been conducted using vaccinia virus, ostensibly for vaccine development. The research has entailed insertion of genes from Venezuelan equine encephalomyelitis virus and from Ebola virus into the vaccinia genome.

Special research was done to find a spot in the vaccinia genome into which foreign genes could be inserted without disrupting viral virulence. (Although vaccinia is not virulent in humans, it is virulent in a number of different animals.) For vaccine development, virulence would not be an issue.

In my opinion, much of this research is of questionable scientific value for anything except biological weapons development. When I juxtapose this research with the closed doors of Russia's military facilities and the fact that certain Russian government factions seem to be returning to Cold-War rhetoric, I am convinced that Russia's biological weapons program has not been completely dismantled. Again, this represents just one set of the indicators in the published literature that arouse my concern.

Proliferation of Russia's biological weapons expertise

There are numerous ways in which Russia's biological weapons expertise can be proliferated to other countries. The most obvious is the departure of Russian experts to other countries. I have contacts in the U.S. who maintain connections with these Russian scientists, and through these contacts I have learned of the pitiful state of these experts. The

Russian government has long been short of funds, and the biotechnology arena is not unaffected. Many of these scientists are unemployed; those that are employed are generally paid poorly or not at all. Some of them have been forced to turn to other lines of work, such as street vending. It is therefore not surprising that some of them would seek to emigrate. In addition, I know of about twenty scientists who formerly worked for the Soviet biological weapons program and who now live in the U.S. This indicates to me that it has been relatively easy for these experts to leave Russia, and if twenty of them are in the U.S., undoubtedly a number of them are in other countries as well.

A second possibility is the sale of technology or equipment to other countries, either by the Russian government or its proxies, or by renegade scientists. As an example of the former, consider the recent allegations in the attached Washington Post article of negotiations between the Russians and the Iraqis for sale of fermenters allegedly designed for single-cell protein production, used for animal fodder. Other information sources have even listed the names of the Russian and Iraqi representatives that participated in these negotiations.

There is no doubt in my mind that these fermenters were destined for use in biological weapons production. First of all, Iraq has used the guise of single-cell protein production as a cover for biological weapons facilities in the past. Second, the particular fermenter size involved in this proposed sale would not be suitable for efficient single-cell protein production. In fact, the resultant product would be prohibitively expensive.

As an example of the sale of technology by renegade scientists, I have a copy of a flier advertising the wares of a company called "BIOEFFECT Ltd," with offices in Moscow and Vienna. The text of this flier is attached. The flier offers recombinant Francisella tularensis bacteria with altered virulence genes. Ostensibly, these organisms are being offered for vaccine production; the flier also notes that they can be used as genetic recipients and to create recombinant microorganisms of biologically active agents. The authors of the flier also express willingness to form cooperative ventures to which they will contribute their genetic engineering knowledge. It is clear from this flier that the scientists of "BIOEFFECT Ltd" are willing to sell their genetic engineering knowledge to anyone.

Another example of the sale of biotechnology knowledge was recently reported in the Russian monthly newspaper "Top Secret". The paper reports that a highly placed employee of the Russian biological

weapons apparatus recently offered his services to the Chinese embassy. Although I have no way to confirm this report, the scenario seems plausible to me.

Yet another mode of proliferation is one that appears at first completely innocuous: scientific publications. Certainly, neither the authors nor the journals stand to gain financially from this type of technology transfer. However, considerable information that can at best be considered dual-use in nature can be found in such open publications. For example, a recent article detailed a method for cultivating Marburg virus. This method is so simple, and requires so little equipment and training, that it could easily be adopted by a terrorist group. Other, more sophisticated types of information published include such things as genetic engineering methods, antibiotic resistant strains of pathogenic microorganisms, and so on.

What is the potential impact of terrorist use of biological weapons?

While we should not ignore the continuing threat of military use of biological weapons, we are not at present poised for war with any nation known or suspected to possess biological weapons (with the possible exception of Iraq). A more likely threat is that posed by the terrorist use of biological weapons. Terrorist use can occur on the level of state-sponsored terrorism; on the level of a large, independent organization like the Aum Shinrikyo cult in Japan; or on the level of an individual acting alone or in concert with a small organization, such as a militia. For these three types of terrorist attack, the expected impact will differ considerably.

There is no doubt, however, that the potential impact is great. A report published by the Centers for Disease Control in April, 1997 evaluated the economic impact of a bioterrorist attack for each of three different biological agents: anthrax, brucellosis, and tularemia. Their model showed that the expected economic impact from such an attack would range from $477.7 million to $26.2 billion per 100,000 persons exposed. A copy of this report is attached.

Furthermore, there is no doubt that we will see future uses of biological weapons by terrorist groups, as there have been several attempts already. One incident, in 1984, involved members of the Rajneeshee cult contaminating restaurant salad bars in Oregon with salmonella, sickening 751 people. Another involved the Aum Shinrikyo cult in Japan. Although best known for its attack in the Japanese subway system in 1995, the cult also attempted to release anthrax from the rooftop of a Tokyo building in 1993. No casualties resulted, but had the

cult better understood the air flow dynamics in a city and released the spores at a different time during the day, the results might have been quite different.

Our general preparedness for military and terrorist biological attacks

Fortunately, in the course of the past four or so years, our preparedness for military and terrorist biological attacks has changed considerably for the better. Heightened awareness of the biological threat has lead to a number of positive developments, such as:

creation of extensive databases containing reference information on biological weapons characteristics

design and development of biological agent detection equipment

analysis of possible attack scenarios and their consequences

development of new, and revision of existing, manuals and handbooks

conduct of intensive training of those would serve as first responders to a biological attack.

However, my analysis of several recently issued handbooks for military use indicated that there were still a considerable number of substantive inaccuracies. Thus, further revisions are necessary for these handbooks.

In my opinion, these inaccuracies largely stem from lack of knowledge. Since the U.S. stopped all offensive biological weapons research in 1969 and significantly curtailed its defensive research until 1994, U.S. knowledge of biological weapons is obsolete in many respects. Only in the last few years has there been a concerted attempt to "catch up." We must continue our recently renewed efforts to understand biological weapons and to analyze the actual threat they present.

Our medical preparedness for military and terrorist biological attacks

The ultimate goal of bio-defense, including all of the defensive steps outlined in the previous section, is to prevent suffering and loss of life, thereby rendering biological weapons ineffective. However, while all of these measures can potentially reduce the suffering and loss of life experienced after a biological attack, they are of limited value without appropriate medical defense. Only the development of appropriate medical urgent prophylaxis and treatment methods can completely eliminate the threat of biological weapons. In its 1997 report on the

possible economic impact of a bioterrorist attack, the CDC notes that, "Rapid implementation of a postattack prophylaxis program is the single most important means of reducing these [economic] losses."

Years of research and development on the medical aspects of bio-defense have resulted in commonly accepted treatment and prophylaxis procedures. These procedures involve three main types of medical defense against biological weapons:

vaccination (treatment before exposure)

urgent prophylaxis (treatment after exposure, but before symptoms arise)

chemotherapy (treatment after onset of illness).

Vaccines, of course, have completely changed the picture of infectious disease on earth. Smallpox has been completely eradicated. A number of other diseases, such as poliomyelitis, that not long ago presented serious threats to humanity have lost their epidemiological significance. Vaccines protect the vaccinated person, making him a "dead end" for the disease, thereby breaking the chain of transmission of the illness (this is true whether the illness is contagious or not). In bio-defense, vaccines can also sometimes be used as urgent prophylactic measures.

The peculiarity of vaccines, though, is that they are extraordinarily specific. In general, a particular vaccine works only against a single illness (occasionally a vaccine will be effective against a few similar illnesses). Use of vaccines in bio-defense will thus be effective when all of the following conditions are met:

The target population is known and limited, i.e. military troops within range of an enemy's arsenal, since it is not realistic to vaccinate everyone in the U.S.

It is known precisely what biological agents are in the enemy's biological weapons arsenal, or the number of possible agents has been narrowed down to a few, since it is impossible to vaccinate troops against every possible biological agent (the role of intelligence is obviously great in making this determination).

The vaccine for the agent(s) has already been developed. Note that for many biological agents, among them glanders, melioidosis, Marburg virus, Ebola virus, and Lassa fever, no vaccine exists.

The biological agents used are not genetically altered strains that would circumvent a vaccine.

Clearly, this is a relatively limited sphere of effectiveness. In the case of most military and all terrorist attacks with biological weapons, vaccines would be of little use. One or more of many possible agents could be used in the weapons, making it virtually impossible to know which agents to vaccinate against. It would also be impossible to determine which portions of the U.S. population are most vulnerable and therefore require vaccination-and yet it would be extremely difficult to vaccinate the entire U.S. Army, not to mention the country's entire population, especially with multiple-dose vaccines. And again, there are many highly hazardous diseases for which vaccines have not even been developed.

Therefore, we cannot rely exclusively or even primarily on vaccination for medical bio-defense. We must also ensure that means for urgent prophylaxis and treatment of these diseases are available as well.

The concept of using drugs for urgent prophylaxis and treatment is not new. However, a number of the existing drugs that could be useful are not available in sufficient quantities or in some cases (such as Marboran, for urgent prophylaxis of smallpox) are not manufactured at all. In addition, drug protocols have not been developed for many of the agents that can be found in biological weapons.

However, using our current understanding of disease etiology and pathogenesis, as well as modern biotechnology and pharmacology, we can rectify this situation. Here is an example of possible new treatment techniques for anthrax, for which there is currently no satisfactory treatment.

The pulmonary form of anthrax caused by biological weapons has a fatality rate that can reach 90%. In this form of anthrax infection, the pathogen enters the lungs and from there passes into the lymph system, via which it is disseminated throughout the body. Death occurs as a consequence of secondary hemorrhagic pneumonia from the effect of toxin produced by the bacteria on lung capillaries. Analysis of the pathogenesis of anthrax has shown that most of the infectious propagation takes place in the lymph system, while infection of the circulatory system is secondary.

The usual form of treatment is a combination of streptomycin and penicillin. However, this treatment is largely ineffective. The problem appears to be that the usual methods of antibiotic administration (intramuscular, subcutaneous, intravenous) utilize the bloodstream.

However, this is not where the main bacterial activity is occurring. Although the antibiotics do reach the lymph system, the concentration is lower than that in the circulatory system, and it drops off more rapidly between doses. At the same time, the immune system is suppressed while the bacteria are propagating in the lymph system. The main cause of death is the toxin produced by the bacteria.

Thus, there are several elements in this process that can be targeted for study. The first is to find ways to modulate the immune system, to counter the immunosuppressive effects of bacterial propagation in the lymph system. The second is to examine ways to increase and maintain the concentration of antibiotic in the lymph system, such as lymphotrophic administration of the drugs. A third possibility is to find a way to destroy the bacterial toxin when it is released, using proteolytic enzymes. The knowledge gained from such research would also have value in treating other infectious diseases that are not related to biological weapons.

I feel strongly that we must devote additional resources to the medical aspects of bio-defense. To illustrate the scale of our current efforts, consider that at the one U.S. organization conducting medical research on anthrax, the U.S. Army Medical Research Institute for Infectious Diseases, two or three people are devoted to this effort full-time. For comparison, consider that at the height of the USSR's biological weapons program, more than 2,000 people were conducting anthrax research (both offensive and defensive). As another example, the USSR had more institutes dedicated to plague research than the U.S. has scientists devoted to the same topic.

Conclusions and Recommendations

Since the primary goal of developing bio-defense is to save human lives, we must greatly increase our efforts to develop new treatment and urgent prophylaxis techniques. As part of this medical research, we must consider a new approach in this area: fundamental research and development of methods for non-specific defense, based on amplifying the immune response of the human body to invasion by any foreign agent.

These efforts, as well as the funds spent on research and development, will pay for themselves many times over. In addition to contributing to our nation's preparedness for a biological attack, they will provide a much-needed push in the treatment of infectious diseases that occur under natural conditions. Infectious diseases remain one of the leading causes of death in the world and cause tremendous losses, in terms of both money and human lives, every year. Furthermore, this

research, especially that into methods for non-specific defense, will also contribute to the treatment of many other types of diseases, such as autoimmune disorders and cancer.

The most suitable approach to this issue would be to significantly increase the research conducted in this area. One possibility would be to establish a medical research center specifically for this purpose.

Such a medical research center would also provide one option for addressing certain non-proliferation concerns. The center could employ Russian scientists who participated in the development of biological weapons, and are currently under- or unemployed, to conduct medical research for the U.S. bio-defense program. In this way, we can ensure that the knowledge of the "graduates" of the most sophisticated biological weapons program in the world is put to peaceful use, and we stand to reap the benefits of their extensive experience.

Another important aspect of our bio-defense program is the continuous analysis of possible routes for biological weapons development. This analysis must cover everything from new biological agents to new delivery means. The focus of such analysis is to identify the threat as clearly as possible in order to focus our medical research and other bio-defense efforts as accurately as possible. Conversely, we can avoid wasting time and resources developing defense against a nonexistent threat.

Finally, several more areas require our continued attention to round out our readiness for biological attack:

- creation of manuals for those who will respond to bio-terrorism incidents
- revision of existing manuals for military physicians
- creation of practical means for defense against possible unusual variants of biological weapons.

Addressing these requirements-medical research, threat analysis, manual revision and defense against unusual biological weapons variants-will greatly enhance U.S. preparedness for a biological attack.

Perspective

The Economic Impact of a Bioterrorist Attack: Are Prevention and Postattack Intervention Programs Justifiable?

Arnold F. Kaufmann, Martin I. Meltzer, and George P. Schmid
Centers for Disease Control and Prevention, Atlanta, Georgia, USA

Understanding and quantifying the impact of a bioterrorist attack are essential in developing public health preparedness for such an attack. We constructed a model that compares the impact of three classic agents of biologic warfare (*Bacillus anthracis*, *Brucella melitensis*, and *Francisella tularensis*) when released as aerosols in the suburb of a major city. The model shows that the economic impact of a bioterrorist attack can range from an estimated $477.7 million per 100,000 persons exposed (brucellosis scenario) to $26.2 billion per 100,000 persons exposed (anthrax scenario). Rapid implementation of a postattack prophylaxis program is the single most important means of reducing these losses. By using an insurance analogy, our model provides economic justification for preparedness measures.

Bioterrorism and its potential for mass destruction have been subjects of increasing international concern. Approximately 17 countries (including five implicated as sponsors of international terrorism) may have active research and development programs for biologic weapons (1). Moreover, groups and individuals with grievances against the government or society have been known to use or plan to use biologic weapons to further personal causes.

Only modest microbiologic skills are needed to produce and effectively use biologic weapons. The greatest, but not insurmountable, hurdle in such an endeavor may be gaining access to a virulent strain of the desired agent. Production costs are low, and aerosol dispersal equipment from commercial sources can be adapted for biologic weapon dissemination. Bioterrorists operating in a civilian environment have relative freedom of movement, which could allow them to use freshly grown microbial suspensions (storage reduces viability and virulence). Moreover, bioterrorists may not be constrained by the need for precise targeting or predictable results.

The impact of a bioterrorist attack depends on the specific agent or toxin used, the method and efficiency of dispersal, the population exposed, the level of immunity in the population, the availability of effective postexposure and/or therapeutic regimens, and the potential for secondary transmission. Understanding and quantifying the impact of a bioterrorist attack are essential to developing an effective response. Therefore, we have analyzed the comparative impact of three classic biologic warfare agents (*Bacillus anthracis*, *Brucella melitensis*, and *Francisella tularensis*) when released as aerosols in the suburbs of a major city and compared the benefits of systematic intervention with the costs of increased disease incidence (from the economic point of view used in society).

Address for correspondence: Martin I. Meltzer, Mail Stop C-12, National Center for Infectious Diseases, Centers for Disease Control and Prevention, Atlanta, GA 30333; fax: 404-639-3039; e-mail: qzm4@cdc.gov.

Analytic Approach

Scenario Assumptions

We compared the impact of a theoretical bioterrorist attack on a suburb of a major city, with 100,000 population exposed in the target area. The attack was made by generating an aerosol of an agent (*B. anthracis* spores, *B. melitensis*, or *F. tularensis*) along a line across the direction of the prevailing wind. The meteorologic conditions (thermal stability, relative humidity, wind direction and speed) were assumed to be optimal (2), and the aerosol cloud passed over the

target area within 2 hours. We projected impact on the basis of 10% and 100% of the target population being exposed to the aerosol cloud.

We assumed that, when inhaled, the infectious dose$_{50}$ (ID_{50}) was 20,000 spores for *B. anthracis* and 1,000 vegetative cells for *B. melitensis* and *F. tularensis*. The rate of physical decay for airborne particles 5 μm or less in diameter was estimated to be negligible during the 2-hour transit time. The rate of biologic decay of the particulate agents was estimated to be negligible for the *B. anthracis* spores and 2% per minute for the *B. melitensis* and *F. tularensis* vegetative cells. Viability and virulence did not dissociate. Persons who were exposed to the *B. anthracis* cloud at any point during the 2-hour transit time inhaled one ID_{50} dose, and persons who were exposed to either the *B. melitensis* or *F. tularensis* cloud inhaled one to 10 ID_{50} doses, depending on their proximity to the origination point of the aerosol cloud.

The epidemic curve for anthrax by days after exposure was assumed to be <1 day, 0% of cases; 1 day, 5%; 2 days, 20%; 3 days, 35%; 4 days, 20%; 5 days, 10%; 6 days, 5%; and 7 or more days, 5% (3-5). Case-fatality rates were also assumed to vary by the day symptoms were first noted. The case-fatality rate was estimated as 85% for patients with symptoms on day 1; 80% for patients with symptoms on day 2; 70% for those with symptoms on day 3; 50% for those with symptoms on days 4, 5, and 6; and 70% for those with symptoms on and after day 7. The increased death rate in persons with an incubation period of 7 or more days is calculated on an assumption of delayed diagnosis, with resultant delayed therapy.

When estimating days in hospital and outpatient visits due to infection, we assumed that 95% of anthrax patients were hospitalized, with a mean stay of 7 days. Patients not admitted to a hospital had an average of seven outpatient visits, and surviving hospitalized patients had two outpatient visits after discharge from the hospital. Persons who received only outpatient care were treated for 28 days with either oral ciprofloxacin or doxycycline. No significant long-term sequelae resulted from the primary infection, and no relapses occurred.

The epidemic curve for brucellosis by days after exposure was assumed to be 0 to 7 days, 4% of cases; 8 to 14 days, 6%; 15 to 28 days, 14%; 29 to 56 days, 40%; 57 to 112 days, 26%, and 113 or more days, 10% (4, 6-9). The case-fatality rate was estimated to be 0.5%. Fifty percent of patients were hospitalized, with an average stay of 7 days. Nonhospitalized patients had an average of 14 outpatient visits, and hospitalized patients had seven outpatient visits after discharge from the hospital. Outpatients received a combination of oral doxycycline for 42 days and parenteral gentamicin for the first 7 days of therapy. Five percent of patients had a relapse or long-term sequelae, and required 14 outpatient visits within 1 year.

The epidemic curve for tularemia by days after exposure was assumed to be: <1 day, 0% of cases; 1 day, 1%; 2 days, 15%; 3 days, 45%; 4 days, 25%; 5 days, 10%; 6 days, 3%; and 7 or more days, 1% (4,10-11). The estimated case-fatality rate was 7.5%; and 95% of patients were hospitalized, with an average stay of 10 days. Nonhospitalized patients had an average of 12 outpatient visits, and hospitalized patients who survived the acute illness had two outpatient visits after discharge from the hospital. Outpatients received oral doxycycline for 14 days and parenteral gentamicin for 7 days. Five percent of patients had a relapse or long-term sequelae and required an average of 12 outpatient visits.

The efficacy of intervention strategies is unknown; our projections are our best estimates based on published clinical and experimental data (4,12-14). For anthrax, the projected intervention program was either a 28-day course of oral ciprofloxacin or doxycycline (assumed to be 90% effective), or a 28-day course of oral ciprofloxacin or doxycycline plus three doses of the human anthrax vaccine (assumed to be 95% effective); for brucellosis, a 42-day course of oral doxycycline and rifampin (assumed to be 80% effective), or a 42-day course of oral doxycycline, plus 7 days of parenteral gentamicin (assumed to be 95% effective); for tularemia, the intervention program was a 14-day course of oral doxycycline (assumed to be 80% effective), or a 14-day course of oral doxycycline plus 7 days of parenteral gentamicin (assumed to be 95% effective). Only 90% of persons exposed in the target area were assumed to effectively participate in any intervention program. Because the target area cannot be precisely defined, we estimated that for every exposed person participating in the intervention program, an additional 5, 10, or 15 nonexposed persons would also participate.

Economic Analyses of Postattack Intervention

To analyze the economic factors involved in establishing an intervention program, we compared the costs to the potential savings from such an intervention. Following the recommendation of the Panel of Cost-Effectiveness in Health and Medicine (PCEHM), we used estimates of actual costs rather than financial charges or market prices, which usually incorporate profit (15). We calculated the net savings (cost reductions) by using the following formula: Net savings = (number of deaths averted x present value of expected future earnings) + (number of days of hospitalization averted x cost of hospitalization) + (number of outpatient visits averted x cost of outpatient visits) - cost of intervention.

When we calculated the costs of hospitalization and outpatient visits, we assumed that only persons with symptoms (i.e., case-patients) would use medical facilities. The remainder of the exposed and potentially exposed populace would receive postexposure prophylaxis.

Present Value of Expected Future Earnings

The cost of a premature human death was nominally valued at the present value of expected future earnings and housekeeping services, weighted by the age and sex composition of the work force in the United States (16). The undiscounted average of future earnings is $1,688,595. As recommended by PCEHM (17), the stream of future earnings was discounted at 3% and 5%, to give values of $790,440 and $544,160, respectively. The present value of expected future earnings was estimated with 1990 dollars, adjusted for a 1% annual growth in productivity (16). However, in constant terms (1982 dollars), the average hourly earnings in private industry fell from $7.52 in 1990 to $7.40 in 1994 (18); therefore, the estimate of future earnings was not adjusted upwards.

Cost of Hospitalization

In 1993, the average charge for a single day of hospitalization was $875 (19). To derive true cost, we multiplied the average charge by the cost-to-charge ratio of 0.635, (the April 1994 statewide average cost-to-charge ratio for urban hospitals in New York state) (16). On this basis, we estimated true hospitalization costs at $556/day (Table 1). Hospital costs included all professional services, drugs, x-rays, and laboratory tests. Lost productivity during hospital stay was valued at $65/day (the value of an "unspecified" day's earnings, weighted for age and sex composition of the U.S. work force) (16).

Cost of Posthospitalization Outpatient Visits

After discharge from the hospital, a patient was assumed to have follow-up outpatient visits, the number of which varied by disease (Table 1). Outpatient visit costs were valued by using the Medicare National Average Allowance (20), which was chosen to represent the equivalent of bulk purchase discounted costs (i.e., actual costs) (Table 1). The first visit has a Current Procedural Terminology (CPT) code of 99201, which is classified as a "level 1" visit, requiring a physician to spend an average of 10 minutes with a patient (20). Subsequent level 1 visits, with the physician spending an average of 5 minutes with each patient, have a CPT code of 99211 (20). During outpatient visits, a general health panel test incorporating clinical chemistry tests and complete blood counts (CPT code 80050) and a single antigen or antibody detection test (e.g., CPT code 86558) were assumed to be ordered (20). Although data on Medicare allowances for office visits and many other procedures were available, data on Medicare allowances for laboratory tests were not. Thus, to establish the costs of the tests, we arbitrarily divided the lowest allowable charge for each test in half. X-rays (CPT code 71021) were valued according to the Medicare National Average Allowance (Table 1). In terms of lost productivity, we assumed that each outpatient visit cost the equivalent of 2 hours, or one-quarter, of the value of an unspecified day (16).

Cost of Outpatient Visits of Nonhospitalized Patients

For nonhospitalized outpatients, the cost of each visit, laboratory test, x-ray, and lost productivity was the same as an outpatient visit for discharged hospital patients and varied by disease (Table 1). We assumed that one set of laboratory tests would be ordered every other visit and that two sets of x-rays (CPT code 71021) would be ordered during the therapeutic course. Drug costs are discussed below.

Cost of an Intervention

The costs of an intervention can be expressed as follows: Cost of intervention = (cost of drugs used) x ([number of people exposed x multiplication

Table 1. Costs of hospitalization and outpatient visits (OPVs) following a bioterrorist attack

	Anthrax		Tularemia		Brucellosis	
	Base	Upper	Base	Upper	Base	Upper
Hospitalized patient						
Days in hospital	7	7	10	10	7	7
Cost per day ($)[a]	556	669	556	669	556	669
Lost productivity ($/day)	65	65	65	65	65	65
Follow-up OPVs (no.)	2	2	2	2	7	7
Cost 1st OPV ($)	28	44	28	44	28	44
Cost other OPVs, ea. ($)	13	24	13	24	13	24
OPV laboratory ($)[b,c]	87	174	87	174	131	261
OPV x-rays costs ($)[d]	66	66	0	0	0	0
Lost productivity ($/OPV)[e]	16	16	16	16	16	16
Total costs ($)	4,541	5,380	6,338	7,582	4,584	5,587
Avg. costs/day ($/day)	649	769	634	758	655	798
% increase: Base to upper estimate		*18*		*20*		*22*
Nonhospitalized patient						
Number of OPVs	7	7	12	12	14	14
Cost 1st OPV ($)	28	44	28	44	28	44
Cost other OPVs, ea. ($)	13	24	13	24	13	24
Lost productivity ($/OPV)[e]	16	16	16	16	16	16
Laboratory costs ($)[b,f]	131	174	261	522	261	522
X-ray costs ($)[d]	66	66	66	66	66	66
Drugs used[g]	D	C	D+G	D+G	D+R	D+R+G
Cost of drugs ($)	6	181	29	29	220	246
Total costs ($)	422	810	722	1,120	972	1,418
Avg. costs/day ($/day)	60	116	60	93	69	101
% increase: Base to upper estimate		*93*		*55*		*46*

Notes: All costs rounded to the nearest whole dollar.
[a]Hospital costs assumed to include all costs such as drugs, laboratory tests, and x-rays.
[b]Laboratory tests consists of general health panel (CPT code 80050) and an antigen or antibody test (modeled on the cost of a *Streptococcus* screen, CPT code 86588).
[c]Follow-up OPVs for hospitalized patients included two laboratory test sets for anthrax and tularemia patients and three laboratory test sets for brucellosis patients.
[d]X-ray costs (CPT code 71021), included two sets taken at different OPVs.
[e]Productivity lost due to an OPV was assumed to be one-quarter of an unspecified day's value.
[f]For OPVs of nonhospitalized patients, one set of laboratory tests is assumed for every two visits.
[g]Drugs used: D = doxycycline; C = ciprofloxacin; R = rifampin.
Sources: See text for explanation of sources of cost estimates.

factor] - number killed - number hospitalized - number of persons who require outpatient visits).

The intervention costs per person depend directly on the costs of the antimicrobial agents and vaccines used in a prophylaxis program (Table 2). We obtained drug prices from the 1996 Drug Topics Red Book and used the lowest cost available for each drug (21). The cost of doxycycline ($0.22 per 200 mg total daily dose) was the Health Care Financing Administration cost, whereas the cost of gentamicin ($3.76 per 160 mg total daily dose), ciprofloxacin ($3.70 per 1,000 mg total daily dose), and rifampin ($5.01 per 900 mg total daily dose) were wholesale costs from pharmaceutical companies. The cost of anthrax vaccine was $3.70 per dose (Helen Miller-Scott, pers. comm., 1996). The cost of administering one vaccine dose or gentamicin injection was estimated at $10.00, on the basis of the 1992 cost of administering a vaccine in a clinical setting (Valerie Kokor, pers. comm., 1996). In estimating the cost of administering oral antimicrobial agents, we assumed weekly visits, during which the drug would be distributed and counseling would be given ($15.00 for the first visit and $10.00 for each subsequent visit).

We assumed that more people would receive prophylaxis than were actually exposed because of general anxiety and uncertainty about the boundaries of the attack, the timing of the attack, and the time it would take nonresidents to travel through the attack area. Three different multiplication factors (5, 10, and 15) were used to construct

Table 2. Costs of prophylaxis following a bioterrorist attack

Level of effectiveness	Anthrax	Tularemia	Brucellosis
Lower			
Effectiveness (%)	90	80	80
Drugs used[a]	D or C	D	D+R
Cost of drugs ($)[b]	6 or 181	3	220
No. of visits[c]	4	2	6
Total cost/ person ($)	51 or 226	28	285
Upper			
Effectiveness (%)	95	95	95
Drugs used[a]	D+V or C+V	D+G	D+G
Cost of drugs ($)[b]	17 or 193	29	36
No. of visits[c]	4	7	12
Total cost/ person ($)	62 or 238	104	161
Minimum No. participants[d]	451,912	418,094	423,440
Maximum No. participants[e]	1,492,750	1,488,037	1,488,037

Notes: All costs are rounded to the nearest whole dollar.
[a]Drugs used: D = doxycycline; C = ciprofloxacin; V = anthrax vaccine; G = gentamicin; R = rifampin.
[b]See text for explanation of drug costs.
[c]Cost of visit to drug-dispensing site: 1st visit = $15/person; follow-up visits = $10/person/visit.
[d]Estimate assumed that the prophylaxis program was initiated on postattack day 6 for anthrax and tularemia and postattack day 113 for brucellosis, that the prophylaxis program had the lower effectiveness level, and that the multiplication factor for unnecessary prophylaxis givn to unexposed persons was 5.
[e]Estimate assumed that prophylaxis was initiated on postattack day 0 (day of release), that prophylaxis had the upper effectiveness level, and that the multiplication factor for unnecessary prophylaxis given to unexposed persons was 15.

alternative cost-of-intervention scenarios that take into account persons who were not at risk but participated in the prophylaxis program. Thus, if 100,000 people were exposed, we assumed that the maximum number seeking prophylaxis was 500,000, 1,000,000, or 1,500,000.

Economic Analysis of Preparedness: Insurance

The analyses outlined above consider only the economics of an intervention after an attack and include several assumptions: First, stockpiles of drugs, vaccines, and other medical supplies would be available and could be rapidly moved to points of need. Second, civil, military, and other organizations would be in place and have the capability to rapidly identify the agent, dispense drugs, treat patients, and keep order within the population. Finally, ongoing intelligence gathering would detect possible bioterrorist threats. The cost of these prerequisite activities can be calculated if they are seen as a form of insurance, the goal of which is to "purchase" the maximum net savings through preparedness to manage the consequences of an attack and reduce the probability of an attack. The "actuarially fair premium" for the "insurance" can be defined as follows (22): Actuarially fair premium = reduction of loss probability x value of avoidable loss.

The term "reduc ion of loss probability" indicates that, although increased surveillance and related activities can reduce the odds of an attack, they cannot guarantee absolute protection. The term "avoidable loss" refers to the fact that, even if a postexposure prophylaxis program were implemented on the day of release (day zero), some deaths, hospitalizations, and outpatient visits would be unavoidable.

Various reductions of attack probability illustrated the impact of these estimates on the calculation of actuarially fair premiums. Such reductions included reducing the probability from 1 in 100 years (0.01) to 1 in 1,000 years (0.001), a reduction of 0.009, and reducing a probability from 1 in a 100 years (0.01) to 1 in 10,000 years (0.0001), and from 1 in 100 years (0.01) to 1 in 100,000 years (0.00001). The attack probability of 0.01 in the absence of enhanced preventive actions was selected for illustrative purposes and does not represent an official estimate.

A range of minimum and maximum values of avoidable loss was derived from the net savings calculations. The values reflect differences in effectiveness of the various prophylaxis regimens, the reduced impact of delayed prophylaxis on illness and death, and the two discount rates used to calculate the present value of earnings lost because of death.

Sensitivity Analyses

In addition to the scenarios discussed above, three sensitivity analyses were conducted. First, the impact of increasing the cost of hospitalization and outpatient visits was assessed by using a set of upper estimates (Table 1). The cost of a hospital day was increased to $669 by increasing the cost-to-charge ratio from 0.634 to 0.764 (the ratio for Maryland) (16). The costs of outpatient visits (first and follow-up) were increased by assuming each visit was a "level 2" visit, doubling the average time a physician spends with each patient. The

costs of laboratory tests were increased to the full amount of the allowable charge (20).

The second sensitivity analysis considered a reduced impact, in which only 10% of the original 100,000 target population were considered exposed. All other estimates were held constant. The third sensitivity analysis considered the threshold cost of an intervention, given differences due to the effectiveness of various drug regimens, and discount rates used to calculate the present value of expected lifetime earnings lost to a death. The threshold cost occurs when net savings equal $0. Thus, the threshold value represents the maximum that could be spent per person on an intervention without having the intervention cost more than the loss from no intervention.

Findings

Postattack Illness and Death

In our model, all three biologic agents would cause high rates of illness and death. In the absence of an intervention program for the 100,000 persons exposed, the *B. anthracis* cloud would result in 50,000 cases of inhalation anthrax, with 32,875 deaths; the *F. tularensis* cloud in 82,500 cases of pneumonic or typhoidal tularemia, with 6,188 deaths; and the *B. melitensis* cloud in 82,500 cases of brucellosis requiring extended therapy, with 413 deaths.

The speed with which a postattack intervention program can be effectively implemented is critical to its success (Figure 1). For diseases with short incubation periods such as anthrax and tularemia, a prophylaxis program must be instituted within 72 hours of exposure to prevent the maximum number of deaths, hospital days, and outpatient visits (Figure 1). Some benefit, however, can be obtained even if prophylaxis is begun as late as day 6 after exposure. The relative clinical efficacy of the intervention regimen has a lesser but definite impact on observed illness and death rates (Figure 1).

A disease with a long incubation period such as brucellosis has a similar pattern (Figure 1); an important difference is the time available to implement an intervention program. Having more time available to implement an intervention program can make a marked difference in its effectiveness. However, the prolonged incubation period creates a greater potential for panic in potentially exposed persons because of the uncertainty about their health status.

Economic Analyses of Postattack Intervention: No Program

Without a postexposure prophylaxis program, an attack with *B. anthracis* is far costlier than attacks with *F. tularensis* or *B. melitensis* (Table 3). The differences between agents in medical costs as a percentage of total estimated costs are due to the large differences in death rates attributed to each agent (Figure 1).

Net Savings Due to a Postexposure Prophylaxis Program

If the postexposure prophylaxis program is initiated early, it reduces the economic impact of all three diseases, especially anthrax (Figure 2). Regardless of drug costs, the largest cost reductions

Table 3. Costs[a] ($ millions) of a bioterrorist attack with no postexposure prophylaxis program

	Anthrax	Tularemia	Brucellosis
Direct costs			
Medical: Base estimates[b]			
Hospital	194.1	445.8	170.3
OPV[c]	2.0	10.5	48.9
Medical: Upper estimates[d]			
Hospital	237.1	543.3	211.7
OPV[c]	4.4	18.5	78.3
Lost productivity			
Illness[e]			
Hospital	21.6	50.9	18.8
OPV[c]	0.7	3.9	15.0
Death			
3% discount[f]	25,985.7	4,891.2	326.5
5% discount[f]	17,889.3	3,367.3	224.7
Total costs			
Base estimates			
3% discount[f]	26,204.1	5,402.4	579.4
5% discount[f]	18,107.7	3,878.4	477.7
Upper estimates			
3% discount[f]	26,249.7	5,507.9	650.1
5% discount[f]	18,153.1	3,983.9	548.4

[a]Assuming 100,000 exposed.
[b]Medical costs are the costs of hospitalization (which include follow-up outpatient visits) and outpatient visits (Table 1).
[c]OPV = outpatient visits.
[d]Upper estimates calculated with data in Table 1.
[e]Lost productivity due to illness is the value of time spent in hospital and during OPVs (Table 1).
[f]Discount rate applied to calculate the present value of expected future earnings and housekeeping services, weighted by age and sex composition of the United States workforce (16), lost due to premature death.

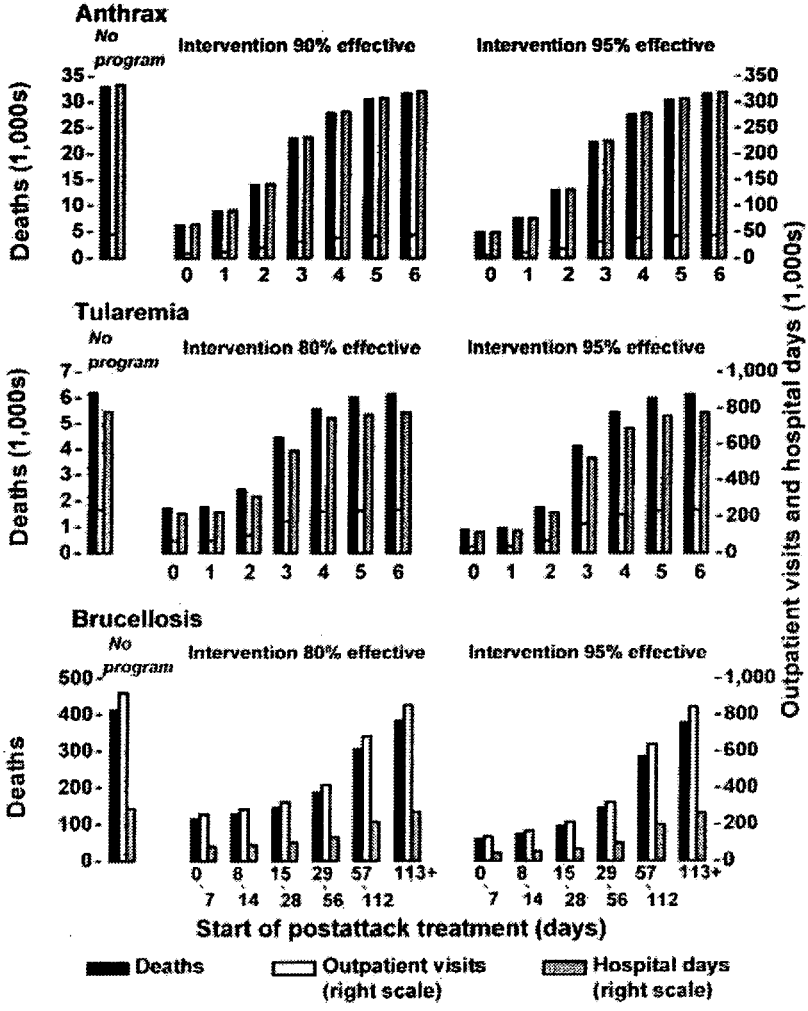

Figure 1. Total deaths, hospital days, and outpatient visits associated with aerosol releases of *B. anthracis*, *B. melitensis*, and *F. tularensis* by the postattack day of prophylaxis initiation and level of prophylaxis effectiveness.

are obtained through a combination of the most effective prophylaxis regimen (i.e., 95% effective, Table 2), the smallest multiplication factor to adjust for persons who unnecessarily receive prophylaxis, and a 3% discount rate to calculate the present value of the expected value of lifetime earnings.

In the case of anthrax, either doxycycline or ciprofloxacin could be used in the intervention program (Table 2), but the use of doxycycline generated the largest savings. The largest difference in net savings between the two drugs was approximately $261.6 million. This difference occurred when it was assumed that the program began on day zero (day of release), each drug was used in combination with the anthrax vaccine, a 3% discount rate was used, and a multiplication factor of 15 for unnecessary prophylaxis was used. This amount is equal to approximately 1.2% of the maximum total net savings generated by using a regimen of doxycycline plus the anthrax vaccine.

Some scenarios, particularly those in which prophylaxis programs were started late, generated negative net savings (i.e., net losses). In the case of tularemia, at a 5% discount rate, net losses of $10.7 to $115.1 million occurred when a postexposure program was delayed until day 6 after exposure, and a prophylaxis regimen of doxycycline and gentamicin (estimated 95% efficacy) was used. For the same scenario, but with a 3% discount, a net savings of $1,513.3 million was observed when a multiplication factor of five for unnecessary prophylaxis was used. However, multiplication factors of 10 and 15 generated net losses of $49.8 and $102.0 million, respectively. With the same drug combination, beginning the program 1 day earlier (day 5 after exposure) resulted in net savings in all scenarios except when a multiplication factor of 15 and a discount rate of 5% were used. Under the latter two assumptions, net savings result only for prophylaxis initiated by day 4 after exposure.

In the case of brucellosis, the use of a doxycycline-rifampin regimen (estimated 80% efficacy), a multiplication factor of 15 for unnecessary prophylaxis, and a discount rate of either 3% or 5% generated net losses regardless of when intervention began (Figure 2). The doxycycline-gentamicin regimen (estimated 95% efficacy) generated net losses only when it was assumed that the start of a program was delayed until 113 or more days after exposure.

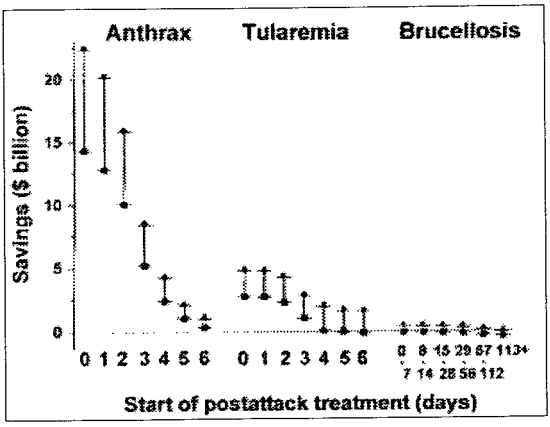

Figure 2. Ranges[a] of net savings due to postattack prophylaxis by disease and day of prophylaxis program initiation.

[a]Maximum savings (●) were calculated by assuming a 95% effectiveness prophylaxis regimen and a 3% discount rate in determining the present value of expected lifetime earnings lost due to premature death (16) and a multiplication factor of 5 to adjust for unnecessary prophylaxis. Minimum savings (■) were calculated by assuming an 80% to 90% effectiveness regimen and a 5% discount rate and a multiplication factor of 15. In tularemia prophylaxis programs initiated on days 4-7 postattack, the minimum savings were calculated by assuming a 95% prophylaxis regimen effectiveness rather than an effectiveness of 80% to 90%.

Preparedness: Insurance

The annual actuarially fair premium that can be justifiably spent on intelligence gathering and other attack prevention measures increases with the probability that a bioterrorist attack can be decreased by such measures (Table 4). However, the potential net savings attributed to reduced probability are minor compared with the potential net savings from implementing a prophylaxis program. Depending on the level of protection that can be achieved, the annual actuarially fair pre-

mium in an anthrax scenario would be $3.2 million to $223.5 million (Table 4). The lower premium would be justifiable for measures that could reduce the risk for an attack from 0.01 to 0.001 and provide the ability to mount an intervention program within 6 days of the attack. The higher premium would be justifiable for measures that could reduce the risk from 0.01 to 0.00001 and allow immediate intervention if an attack occurred.

Sensitivity Analyses

The upper estimates of the cost of hospitalization increased average costs per day by 18% to 22%, and upper estimates of the cost of outpatient visits increased average costs per day by 46% to 93% (Table 1). However, the upper estimates only increased medical costs by 1% to 6% of the total medical costs associated with a bioterrorist attack (Table 3). The largest increase was for brucellosis, for which upper estimates increased medical costs from 38% to 44% of total costs (Table 3).

Table 4. The maximum annual actuarially fair premium[a] by reduction in probability of event and size of avoided loss: Anthrax

		Actuarially fair annual premium ($ millions)		
Days post-attack[b]	Preventable loss ($millions)	0.01 to 0.001	0.01 to 0.0001	0.01 to 0.00001
Maximum loss estimate[c]				
0	22,370.5	201.3	221.5	223.5
1	20,129.4	181.2	199.3	201.1
2	15,881.5	142.9	157.2	158.7
3	8,448.0	76.0	83.6	84.4
4	4,200.1	37.8	41.6	42.0
5	2,076.1	18.7	20.6	20.7
6	1,013.8	9.1	10.0	10.1
Minimum loss estimate[d]				
0	14,372.4	128.9	141.8	143.1
1	12,820.1	115.4	126.9	128.1
2	10,049.1	90.4	99.5	100.4
3	5,200.1	46.8	51.5	51.9
4	2,429.7	21.9	24.1	24.3
5	1,004.2	9.4	10.3	10.4
6	351.2	3.2	3.5	3.5

[a]See text for definition.
[b]No. of days from attack to effective initiation of prophylaxis.
[c]Maximum loss preventable (potential net savings) occurs with the doxycycline-anthrax vaccine prophylaxis regimen, a multiplication factor of 5 for unnecessary prophylaxis, and a discount rate of 3% (Table 2).
[d]Minimum loss preventable (potential net savings) occurs with the ciprofloxacin prophylaxis regimen, a multiplication factor of 15 for unnecessary prophylaxis, and a discount rate of 5% (Table 2).

When the number of persons infected during an attack was reduced tenfold, the patient-related costs were reduced proportionately (Table 3). In most cases, however, the net savings in total costs are less than 10% of the net savings when 100% of the target population was presumed infected. The shortfall in savings is caused by an increase in the number of unexposed persons receiving prophylaxis. In the case of anthrax, when intervention programs are initiated within 3 days of exposure, savings are 4.1% to 10% of those in the original scenario (Figure 2). Delaying initiation of prophylaxis until days 4, 5, or 6 after exposure, however, results in net losses of $13.4 to $283.1 million. Losses occur regardless of prophylaxis regimen, discount rate, or multiplication factor used to adjust for unnecessary prophylaxis by unexposed persons.

In scenarios in which a multiplication factor of 15 was used to adjust for unnecessary prophylaxis, the threshold value of intervention was always above the prophylaxis cost for anthrax but not above the prophylaxis costs for tularemia and brucellosis (Table 5). For tularemia, the threshold intervention costs exceeded disease costs up to day 5 in the scenario with 95% effectiveness and a 5% discount, and for brucellosis, at all levels in the scenarios with 80% effectiveness and up to day 56 in the scenarios with 95% effectiveness. This is consistent with the lower range of estimated net savings (net losses) given in Figure 2. Reducing the number of unexposed persons receiving prophylaxis increases the cost thresholds, making the program cost beneficial. For example, changing the multiplication factors for unnecessary prophylaxis to 5 and 10 increases the cost thresholds to $659 and $319, respectively, for a brucellosis prophylaxis program initiated 15 to 28 days after exposure, with a 5% discount rate. If a discount rate of 3% is used instead of 5%, the cost thresholds increase to $799 and $387. All these cost thresholds are above the estimated prophylaxis cost of $285 per person for the doxycycline-rifampin regimen and $161 per person for the doxycycline-gentamicin regimen (Table 2).

Conclusions

The economic impact of a bioterrorist attack can range from $477.7 million per 100,000 persons exposed in the brucellosis scenario to $26.2 billion per 100,000 persons exposed in the anthrax scenario (Table 3). These are minimum

Table 5. Cost thresholds[a] of interventions ($/person) by day of intervention initiation, prophylaxis effectiveness, and discount rates.

Threshold costs for intervention ($/person, multiplication factor of 15[b])								
Anthrax			Tularemia			Brucellosis		
Post-attack day[d]	Disc. rate[c] 5%	3%	Post-attack day	Disc. rate 5%	3%	Post-attack day	Disc. rate 5%	3%
	90% effectiveness[e]			*80% effectiveness[e]*			*80% effectiveness[e]*	
0	9,838	14,238	0	1,891	2,633	0-7	233*	282*
1	8,851	12,809	1	1,873	2,609	8-14	224*	272*
2	7,022	10,162	2	1,599	2,227	15-28	211*	255*
3	3,775	5,463	3	756	1,053	29-56	179*	217*
4	1,893	2,739	4	258	366	57-112	86*	104*
5	944	1,366	5	79	110	113+	24*	30*
6	468	677	6	20*	28			
Prophylaxis cost[f]		*$226*			*$28*			*$285*
	95% effectiveness[e]			*95% effectiveness[e]*			*95% effectiveness[e]*	
0	10,370	15,007	0	2,229	3,104	0-7	274	333
1	9,359	13,544	1	2,207	3,074	8-14	264	320
2	7,427	10,948	2	1,898	2,644	15-28	248	301
3	3,995	5,782	3	898	1,251	29-56	211	256
4	2,004	2,900	4	328	457	57-112	102*	124*
5	1,000	1,447	5	93*	131	113+	29*	35*
6	496	718	6	23*	32*			
Prophylaxis cost[f]		*$238*			*$104*			*$161*

*Threshold value is below estimated cost of prophylaxis.
[a]Cost threshold is the point where cost of intervention and net savings due to the intervention are equal.
[b]Multiplication factor to adjust for persons who participated in the prophylaxis program but were unexposed.
[c]Applied to present value of expected future earnings and housekeeping services (weighted average for age and sex).
[d]Postattack day on which prophylaxis was effectively implemented.
[e]See Table 2 for prophylaxis regimens assumed to give the stated levels of effectiveness and cost/person of prophylaxis.

estimates. In our analyses, we consistently used low estimates for all factors directly affecting costs. The ID_{50} estimates for the three agents are twofold to 50-fold higher than previously published estimates (5,6,10,11), resulting in a possible understatement of attack rates. Also, in our analyses we did not include a number of other factors (e.g., long-term human illness or animal illnesses) (Table 6) whose cumulative effect would likely increase the economic impact of an attack.

Our model shows that early implementation of a prophylaxis program after an attack is essential. Although the savings achieved by initiating a prophylaxis program on any given day after exposure has a wide range, a clear trend of markedly reduced savings is associated with delay in starting prophylaxis (Figure 2). This trend was found in the analysis of all three agents studied.

Delay in starting a prophylaxis program is the single most important factor for increased losses (reduced net savings). This observation was supported by the actuarially fair premium for preparedness analysis (Table 4). Reductions in preventable loss due to early intervention had significantly greater impact on the amount of an actuarially fair premium than reductions in probability of an attack through intelligence gathering and related activities.

Although implemented at different times in a threat-attack continuum, both attack prevention measures and prophylaxis programs are forms of preventive medicine. Attack prevention measures seek to prevent infection, while prophylaxis programs prevent disease after infection has occurred.

Using an actuarially fair premium analogy in which cost and benefit are required to be equal, we find that the incremental rate of increasing prevention effectiveness (the marginal increase) declines rapidly as probability reduction targets go from 0.001 to 0.0001 to 0.00001. Because the loss probability is decreasing on a logarithmic scale, the potential increment in marginal benefit drops comparably, resulting in ever smaller increments in the protection above the preceding base level.

Conversely, delaying a prophylaxis program for anthrax, a disease with a short incubation

Table 6. Potential factors affecting the economic impact of a bioterrorist attack

Factor	Potential impact on net savings	Relative magnitude of impact
Higher than projected case-fatality rate	Increase	++++
Long term illness (physical and psychological)	Increase	++
Decontamination and disposal of biohazardous waste	Increase	++
Disruptions in commerce (local, national, and international)	Increase	++
Animal illness and death	Increase	+
Lower than projected effectiveness of prophylaxis	Decrease	- - -
Adverse drug reactions due to prophylaxis	Decrease	-
Postattack prophylaxis distribution costs, including crowd control and security	Decrease	-
Training and other skill maintenance costs	Decrease	-
Procurement and storage of antimicrobial drugs and vaccines before attack	Decrease	-
Criminal investigations and court costs	Variable	+/-

period and a high death rate, increases the risk for loss in a manner akin to a semilogarithmic scale. Arithmetic increases in response time buy disproportionate increases in benefit (prevented losses.) The potential for reducing loss is great because an attack is assumed, thus increasing the actuarially fair premium available to prepare for and implement a rapid response.

Large differences between prophylaxis costs and the threshold costs for most scenarios, particularly if prophylaxis is early (Table 5), suggest that the estimates of savings from prophylaxis programs are robust. Even with large increases in prophylaxis cost, net savings would still be achieved.

The ability to rapidly identify persons at risk would also have significant impact on costs. For example, the threshold costs for brucellosis prophylaxis are often lower than intervention costs when the ratio of unexposed to exposed persons in the prophylaxis program is 15:1 (Table 5). This finding provides an economic rationale for preparedness to rapidly and accurately identify the population at risk and reduce unnecessary prophylaxis costs.

The maximum amount of the annual actuarially fair premium varies directly with the level of risk reduction and the rapidity of postattack response (Table 4). The calculated amount of actuarially fair premiums, however, should be considered a lower bound estimate. A higher estimate (called the certainty equivalent) can also be calculated; however, this requires the determination of a social welfare function (22), and such complexity is beyond the scope of this study.

Our model provides an economic rationale for preparedness measures to both reduce the probability of an attack and increase the capability to rapidly respond in the event of an attack. The larger portion of this preparedness budget (insurance premium) should be allocated to measures that enhance rapid response to an attack. These measures would include developing and maintaining laboratory capabilities for both clinical diagnostic testing and environmental sampling, developing and maintaining drug stockpiles, and developing and practicing response plans at the local level. These measures should be developed with a value-added approach. For example, the laboratory capability could be used for other public health activities in addition to preparedness, and drugs nearing their potency expiration date could be used in government-funded health care programs. However, these secondary uses should not undermine the preparedness program's effectiveness.

Arnold Kaufmann is a retired Public Health Service officer, formerly assigned to the National Center for Infectious Diseases.

References

1. Cole LA. The specter of biological weapons. Sci Am 1996;275:60-5.
2. Gochenour WS. Aerobiology. Mil Med 1963;128:86-9.
3. Abramova FAN, Grinberg LM, Yampolskaya OV, Walker DH. Pathology of inhalational anthrax in 42 cases from the Sverdlovsk outbreak of 1979. Proc Natl Acad Sci 1993;90:2291-4.
4. Benenson AS, editor. Control of communicable diseases manual. 16th ed. Washington (DC): American Public Health Association, 1995.
5. Messelson M, Guillemin J, Hugh-Jones M, Langmuir A, Popova I, Shelokov A, et al. The Sverdlosvsk anthrax outbreak of 1979. Science 1994;266:1202-8.
6. Kaufmann AF, Fox MD, Boyce JM, Anderson DC, Potter ME, Martone WJ, et al. Airborne spread of brucellosis. Ann NY Acad Sci 1980;335:105-14.
7. Olle-Goig JE, Canela-Soler J. An outbreak of *Brucella melitensis* infection by airborne transmission among laboratory workers. Am J Public Health 1987;77:335-8.

8. Staszkiewicz J, Lewis CM, Colville J, Zervos M, Band J. Outbreak of *Brucella melitensis* among microbiology laboratory workers in a community hospital. J Clin Microbiol 1991;29:287-90.
9. Trever RW, Cluff LE, Peeler RN, Bennett IL. Brucellosis I. laboratory-acquired acute infection. Arch Intern Med 1959;103:381-97.
10. McCrumb FR. Aerosol infection of man with *Pasteurella tularensis*. Bacteriolical Reviews 1961;25:262-7.
11. Saslaw S, Eigelsbach HT, Wilson HR, Prior JA, Carhart S. Tularemia vaccine study II. respiratory challenge. Arch Intern Med 1961;107:689-701.
12. Friedlander AM, Welkos SL, Pitt MLM, Ezzell JW, Worsham PL, Rose, KJ, et al. Postexposure prophylaxis against experimental inhalation anthrax. J Infect Dis 1993;167:1239-42.
13. Sawyer WD, Dangerfield HG, Hogge AL, Crozier D. Antibiotic prophylaxis and therapy of airborne tularemia. Bacteriolical Reviews 1966;30:542-8.
14. Solera J, Rodriguez-Zapata M, Geijo P, Largo J, Paulino J, Saez L, et al. Doxycycline-rifampin versus doxycycline-streptomycin in treatment of human brucellosis due to *Brucella melitensis*. Antimicrob Agents Chemother 1995;39:2061-7.
15. Luce BR, Manning WG, Siegel JE, Lipscomb J. Estimating costs in cost-effectiveness analysis. In: Gold MR, Siegel JE, Russell LB, Weinstein MC, editors. Cost-effectiveness in health and medicine. New York: Oxford University Press, 1966:176-213.
16. Haddix AC, Teutsch SM, Shaffer PA, Dunet DO, editors. Prevention effectiveness: a guide to decision analysis and economic evaluation. New York: Oxford University Press, 1996.
17. Lipscomb J, Weinstein MC, Torrance GW. Time preference. In: Gold MR, Siegel JE, Russell LB, Weinstein MC, editors. Cost-effectiveness in health and medicine. New York: Oxford University Press, 1966:214-35.
18. U.S. Bureau of the Census. Statistical abstract of the United States: 1995. 115th ed. Washington (DC): U.S. Government Printing Office, 1996.
19. National Center for Health Statistics. Health, United States, 1995. Hyattsville (MD): U.S. Department ofHealth and Human Services, Public Health Service, 1996.
20. HealthCare Consultants of America, Inc. HealthCare Consultants' 1996 physicians fee and coding guide. 6th ed. Augusta (GA): HealthCare Consultants of America, Inc. 1996.
21. Cardinale V, editor. 1996 Drug Topics Red Book. Montvale (NJ): Medical Economics Company, Inc., 1996.
22. Robison LJ, Barry PJ. The competitive firm's response to risk. New York: Macmillan, 1987.

PREPARED STATEMENT OF BRIAN P. FAIRCHILD, BRIAN P. FAIRCHILD AND ASSOCIATES

Economic Considerations

There are myriad dangers and forces arrayed against the United States, which require and justify the existence of the Central Intelligence Agency's Directorate of Operations (DO), also known as the Clandestine Service (CS). As the world's only superpower, leading the world economically, militarily, and technologically, the United States is the natural target of our enemies and our competitors. We face the proliferation of weapons of mass destruction, such as, chemical, biological, and nuclear weapons, and their delivery systems. The threat from these weapons systems is exacerbated by the availability of former Soviet military and scientific personnel, who, in some cases, are currently shopping for jobs among our enemies in the Middle East. In addition, our government is confronted and challenged by the lack of stability in the countries which formerly comprised the Soviet Union, as well as by the potential for a military conflagration in the Middle East, and by the threats from international organized crime and terrorism.

Moreover, in early February 1996, FBI Director Freeh, in a request to Congress for increased legal authority to counter fast growing industrial espionage by friendly and adversarial nations against the U.S., warned that at least 23 nations now make U.S. Industry the prime target of their economic espionage activities.

These threats represent potential economic disaster if they should befall us. The economic loss of an enemy attack on our country, or on our allies, would be in the billions of dollars. The cost from international crime cartels is already estimated to be in the hundreds of millions of dollars, and the damage to our industries by economic espionage has an enormous impact on us, and could be fatal to some of our key, strategic industries.

Unlike the United States, the leaders in many of these nations do not answer to an empowered citizenry, nor are they encumbered by a governmental system of checks and balances. In many of these countries, the will of a single authoritarian ruler, or, at most, a few senior officials, is all that is needed to initiate wide-ranging policies and programs against our country. Often, massive budgets and manpower allocations support these programs.

The CIA, and more specifically, the DO, as our government's first line of defense, can be invaluable in discovering, understanding, and countering these threats. The DO, however, must be provided with the resources to ensure that its officers are well trained and equipped to perform this vital mission. Intelligence collection, however, is not cost effective. To use a medical analogy, intelligence collection is much like health insurance. One pays and pays in the hope that it will never be used, but when one's health is threatened, this investment of resources pays dividends.

The Value of Human Intelligence

When the DO is criticized, the criticism often centers on the value of technical collection over human collection. Many argue that technical intelligence is easier to collect, more accurate, and much more straightforward than human intelligence. Nothing could be further from the truth. The fact of the matter is, because of emerging encryption technologies, technical intelligence has become very difficult, and sometimes, impossible to collect. It is also subject to countermeasures, it is easily used to channel misinformation, and its distance from human foibles, does not recommend it as a superior collection mechanism.

One must always remember that technology is an enabling mechanism - that is, it enables one to perform one's job more expeditiously than one would be able to without it. In other words, it assists one in performing a given function, but it is not the function itself. For example, communication technology allows national leaders to direct their military forces in support of a given policy, but the communication is not the policy itself. It is only data, and that data cannot tell an analyst if information intercepted from a communications network is a major part of the policy, a small portion of the policy, or simply misinformation. Moreover, the data cannot be challenged, queried, or augmented. It simply is what it is. And, of course, some information is not susceptible to technical collection at all. The current unrest in Indonesia is a good example. If policymakers need to know what plans the demonstrators are making, or who among the demonstrators are attempting to organize the masses into a credible organization, only a human source can obtain this information. Such developments are not broadcast over communications networks, nor are they vulnerable to satellite photography.

A well-placed human source, on the other hand, can tell a case officer, not only if the information gathered via technology is misinformation, but he or she can also describe a given policy, and tell how it will unfold. Moreover, a human source can be challenged,

queried, and one can task the source to go back and get more detail. In addition, a human source can augment the intelligence by placing it in perspective, providing an assessment of the leadership, and by describing factional in fighting.

Technical collection can, and does, make a valuable contribution to a particular intelligence requirement, but it can never take the place of a human source. Moreover, the immense amount of money invested in technical collection cannot be maximized if human intelligence is not fully operational. Imagine a situation where signals intelligence and satellite photography indicate that a military action by a hostile power is imminent, but it is unclear if this action is simply a scheduled exercise, or the beginning of a military campaign against a neighboring country. A well-placed human source can often provide critical information which helps answer such questions, thereby placing the technical intelligence in context, and enhancing its value.

While human intelligence is crucial, it is not infallible. The CIA is often criticized for not being able to predict a specific event such as the fall of the Soviet Union, or, most recently, the nuclear test in India. For some reason, some people insist on thinking that an intelligence agency, by the mere virtue of its existence, should be able to answer any question put to it, and if it can't, they accuse it of failure.

This misses the point. It should be obvious that no intelligence agency has a direct line to truth. Intelligence agencies are not omniscient, and no other organizations are held to this standard. People, for example, don't accuse the FBI of failure every time it fails to predict a major move by organized crime, nor do they give up on medical research because a cure for cancer has not been discovered.

While the CIA should be held to a high standard, it should not be held to an irresponsible standard. In a perfect world, the DO would have highly placed sources in every office of every hostile world leader. In reality, however, this is seldom the case. Accurate and timely intelligence on key topics is hard to acquire. Moreover, it takes a great deal of skill and commitment by the DO's men and women, who are frequently in harms way, to recruit and handle sources who can provide such intelligence. We must remember that intelligence is not a panacea, one cannot just snap one's fingers and expect that an intelligence agency can answer any question no matter how difficult. Rather, intelligence is just one piece of the puzzle, often times a critical piece, which enables policymakers to make a better assessment of a policy problem.

The question that needs to be raised is - how much of a contribution does intelligence make, and are the policymakers better off having this information? In the majority of cases, I believe any capable analyst would rather have the input of intelligence than to attempt an assessment of a critical policy problem without it. Sometimes intelligence can provide the one piece of critical information needed, and sometimes it makes little contribution. The majority of the time, however, intelligence provides critical insights into a problem that, while not absolutely definitive, enables a policymaker to come to a reasonable decision.

In the above examples of the fall of the Soviet Union, and the recent nuclear test in India, the fact that the DO did not provide the exact date and time of these events is not the point. These events did not take place in a vacuum. Rather, the question that should be raised is - did the DO provide enough intelligence prior to these events to indicate to policymakers that these events would most likely take place in the not too distant future. Certainly the DO had been reporting on India's nuclear program for years. I know this to be true, because I personally had some experience with this operation. And the DO certainly reported on the state of the Soviet economy, which indicated that the fabric of the former Soviet Empire was unraveling. If however, policymakers had insufficient intelligence to reasonably assess that these important events would occur in the near future, this would be an intelligence failure.

All of the above does not mean, however, that there are no problems within the DO. There are serious problems, and these problems can and must be dealt with. For example, the DO has been criticized for having a culture obsessed with the recruitment of sources, to the detriment of other disciplines such as counterintelligence and operational security. This accusation is true, but it is not hard to understand. The DO is in the espionage business - the recruitment of sources is what the DO does - its raison d'être. This emphasis on recruitment, however, must change in order for the DO to successfully perform its mission.

Unfortunately, discussion of the problems in the CIA and the DO often become sensationalized and used for political purposes. The CIA's problems should be dealt with straight on, with the goal of making this vital organization stronger and better able to meet its mission. The explosion of impassioned and politically motivated criticism every time the CIA makes a real or perceived misstep is a non-starter, and counter productive. The nation needs the CIA, and the CIA needs leadership and support. If its problems are viewed honestly and constructively, our country will be better off, and the national interest will be well served.

Below, I will attempt to explain the problems the DO currently

faces, and then offer possible solutions to these problems. It should be noted, however, that the following addresses only the DO's primary mission - to obtain intelligence information, from human sources, through espionage. While the DO's Paramilitary and Covert Action operations are often highlighted in the press, the DO's main mission, and the one in which almost all of its case officers are engaged, is the acquisition of foreign intelligence sources through espionage.

Directorate of Operations (DO)

Before launching into a detailed explanation of the current problems of the DO, it is important to take a minute to understand what the DO was created and designed to be. The DO was created and designed to be a highly specialized organization, tasked with the mission to obtain select strategic intelligence information, through espionage, for the President and the National Security Council. Because of the adverse impact exposure of our espionage operations would have on our relations with the countries against whom we spy, the scope of the DO was intentionally limited. That is, the DO was chartered to obtain only that strategic information which can not be obtained by any other means, and only that information which is worth the risk of such a potential exposure. To minimize the risk of exposure, the DO was also tasked to protect its operations by initiating a vigorous counterintelligence program, and by using good operational security, known as "tradecraft" within the DO.

The description above makes perfect sense. If one plans to engage in risky ventures, one must ensure that only those ventures worth the risk are undertaken, and that these ventures are protected by all means.

As I will explain below, the mission of the DO is no longer limited to obtaining key strategic intelligence. Rather, the scope of its intelligence collection has been vastly expanded, and this has limited its ability to obtain quality intelligence. In addition, the DO has not maintained a vigorous counterintelligence capability, and its operational security is in disrepair. This, in turn, has affected the morale of the DO's officer corps, which has resulted in a large number of resignations by both junior and veteran case officers. These problems are serious, but they can be fixed.

Operations: The DO's Worldview

Before one can understand how the DO conducts operations overseas, one must understand the DO's world vision. The DO divides the world into two operational environments - a benign environment, and a hostile environment. The DO places all "hard target" countries into the hostile environment. The rest of the world is considered to be a benign

operational environment. There is no doubt that the countries included in the hostile group are correct. The rest of the world, however, is no longer benign, but the DO continues to operate as though it is.

The DO's division of the world into hostile and benign environments is rooted in the history of the Cold War. When CIA was created in 1947, Western Europe was in a shambles, and the rest of the world was made up of developing nations. The cold war was underway, and the world quickly became bi-polar; on one side was the communist monolith comprised of the Soviet Union, China, and its few supporters around the world, and on the other side, was the U.S. and all other countries. If a nation was not in the "Soviet Camp", it was believed to be on our side. To counter the Soviets, the DO moved quickly to establish stations in most countries not siding with the Soviets, and it began a campaign to train, equip, and supply counterintelligence forces around the world in an effort to motivate them to work with the DO against local Soviet targets.

The DO's emphasis on countering the Soviets worldwide is very important to understand. Originally, DO stations were placed in almost every country, not because of U.S. policy interest in those countries per se, but to enable DO officers to target Soviet officials wherever they were assigned. The DO especially sought to obtain the assistance of the host counterintelligence services against the Soviet target, and because it worked so closely with these services for so long, it refused to believe that these services would ever launch offensive operations against it. Many senior DO officers still believe this to be true, and conduct their operations accordingly. In fact, as many of these countries became more independent, they began to differ with U.S. diplomatic, military, and economic positions. In some cases, differences between the U.S. and these countries became hostile, causing the local leadership to order offensive counterintelligence operations against local DO officers and operations.

The DO, however, did not change with the times, and rather than developing new ways of working in these countries, it stood its ground. Even to this day, unless it is operating in an obviously hostile country, the DO conducts its operations as though they face little or no threat of compromise.

This is an area in which the DO requires fixing. To securely recruit and handle sources abroad, an intelligence agency must have intelligence officers, in-country, who are hidden under the mantle of viable cover, and it must know the capabilities of its opponents - the local counterintelligence service (hereafter referred to as the local service) and police force. The intelligence disciplines concerned with obtaining and

exploiting a detailed knowledge of these local services are counterintelligence, and operational security. Unfortunately, the DO has paid little attention to these disciplines, preferring to concentrate its efforts on the recruitment of sources.

Cover

In the late 1940's and early 1950's, when the DO was establishing stations around the world to counter the threat of communism, much of the world was quite undeveloped, with little or no commercial representation. The DO, therefore, naturally placed its stations in U.S. Embassies located in the capital of each country, and sent its officers to these stations under the cover of other government departments. The DO failed to move its stations to other platforms, however, when the political and economic policies in these countries became more independent of, and competitive with, U.S. positions. This fact has had a profound impact on the security of DO operations.

The reason for this impact, is that each U.S. Embassy overseas hires local citizens - Foreign Service Nationals - who staff many of the embassy's most important offices. This ready-made pool of local citizens provides the counterintelligence service with an opportunity to have its staff officers obtain employment, undercover, at the Embassy. It also provides an excellent pool of potential sources, which can be recruited by the local service, or any other intelligence service, to report on the American officers with whom they have contact.

This fact, in tandem with the DO's lack of knowledge of the capabilities of the local counterintelligence services, and its poor operational security (which will be explained below), enables enemy forces to discover which officers within the embassy are undercover DO officers. This situation is commonly accepted by DO case officers and managers overseas, who often say, "cover is a state of mind". This often-used phrase underscores two specific problems - DO officers have little or no viable cover, and the DO continues to operate as though this does not matter.

The lack of attention paid to cover, counterintelligence, and operational security within the DO is highlighted in the following examples:

In two large, important stations to which I was assigned, one in Asia and the other in Europe, the local counterintelligence service made it known to the station that it was aware, almost to a man, of the number of DO undercover officers in the embassy. This fact, notwithstanding, operations continued unchanged.

In the station in Europe, the security of the station, and the identity of its undercover officers, was put at risk by the fact that the station's windows were kept wide open. On a daily basis, my colleagues and I walked in front of these windows, in full view of the local police officers assigned to protect the embassy, as well as the residents of an apartment house located a short distance away. When I asked station managers how they could allow such a security breach, they responded by stating that the station had such a close relationship to the local service, that the local service would never launch offensive operations against it. And, if it did, they said, they were personally so close to their counterparts in the local service, that these officers would warn them of the threat. It was later revealed that, at precisely that time, the local service was, in fact, running an offensive operation against the station.

In the station in Asia, the Chief of Station held staff meetings for all officers once a week in his office. The problem was that the chief's office was constructed with clear windows along its entire length, and these windows faced a number of high-rise buildings. Anyone located in any of those buildings, using a simple pair of low power binoculars, could, at least once a week, observe virtually every DO undercover officer in the embassy.

In the station in Asia, my cover was ostensibly as an officer assigned to the office of another government department. I actually performed work for that office, and for all intents and purposes, I was supposed to be indistinguishable from the real officers. The senior officer of my cover office was even required to submit a fitness report for me each year to maintain my cover. On one occasion, the senior officer was speaking to the Foreign Service National responsible for the embassy's personnel section. The senior officer asked this woman by what date he had to submit my fitness report to her so that it would get back to Washington D.C. by the due date. She appeared a little embarrassed at first, but then regained her composure and said that there was no need for him to submit a fitness report for me, as "Mr. Fairchild is (pause) ahh, complimentary to your office".

Counterintelligence

Counterintelligence is the discipline by which an intelligence agency attempts to thwart the efforts of enemy intelligence agents to commit espionage

One of the most important duties of counterintelligence officers is to recruit spies in the opposition intelligence services. Historically, the DO has done poorly against this target, and as a result, most DO stations

and officers do not know what the local services are doing to discover and counter station operations.

Another crucial responsibility of counterintelligence officers is to root out the spies in its own organization. The recruitment of former DO officer Aldrich Ames, by the Soviet Union, is a perfect example of the value of a counterintelligence operation. In addition to providing the Soviets with the identities of U.S. spies in the Soviet Union, Ames also provided: information on CIA officers and operations (which could be used by the Soviets and later the Russians) in future recruitment operations, detailed information on the DO's method of operation, and reams of intelligence and operational reporting.

A fact that is rarely mentioned, however, is that this case also illuminates one of the DO's great successes - the fact that it had successfully recruited and handled, right under the nose of the KGB, a number of sources in the Soviet Union, all of whom were providing valuable information. Had it not been for the traitor Ames, most of these sources would still be operating on our behalf.

Counterintelligence officers are also crucial in helping to determine if a station's operations have been compromised. They do this by comparing developments in the operation to the known modus operandi of the local services, and by establishing links, via investigation, between the recruited source, and the personnel and associates of the local service. Few resources are expended on developing an investigative capability overseas, therefore, most field stations have little investigative capability.

The reason the DO has done poorly in counterintelligence is because, in the DO, counterintelligence takes a back seat. There is no counterintelligence career track, and while a few officers have spent their careers in the Counterintelligence Staff, later changed to the Counterintelligence Center, the majority of case officers never have a counterintelligence assignment, and have little understanding of what counterintelligence officers do. Overseas, a case officers' counterintelligence duties merely amount to periodically submitting boilerplate reports, which require the officer to subjectively review his or her recruited source, rather than performing a vigorous investigation. Moreover, when officers overseas are posted specifically to a counterintelligence slot, they normally staff an office of one, and are little more than records custodians for the boilerplate reports filed by the case officers.

Operational Security

Operational Security, which overlaps with cover and counter-intelligence, is the discipline by which an intelligence agency attempts to protect its specific operations. Central to this discipline is a detailed knowledge of the capabilities of the counterintelligence and police forces arrayed against it. Armed with this information, techniques can be developed to counter the local service's strengths, while taking advantage of its weaknesses.

For example, an intelligence agency needs to know what kind of physical surveillance capability the local service has, including: the size of its surveillance teams, the kind of vehicles and communications the teams use, whether aircraft, or street mounted cameras are used to augment ground teams, and how it uses its resources to cover the city. In addition, it is vital to know the extent to which the local service monitors telephone calls, as well as its capability to intercept electronic emissions, and to place electronic listening devices in offices and residences.

Because the recruitment of sources is emphasized over the defensive aspects of the job, the DO's "tradecraft", that is, the development and use of techniques to avoid detection by enemy forces, is poorly developed. The truth is, very few case officers have any real knowledge of tradecraft at all. This is because the DO rarely has detailed knowledge of the counterintelligence, and operational security threats arrayed against it. The exception to this rule, is the coverage the DO has of counter-intelligence services in some of the "hard target" countries.

Moreover, because the DO considers most of the world to be a benign operational environment, there is not much interest or concern regarding these threats. Many officers wrongly believe that, because most countries in the world have a symbiotic relationship with the United States, they would not jeopardize their relationship with our country by launching offensive operations against station operations. Other officers say that as long as nothing adverse happens while they are in-country, they do not care if the local counterintelligence service has compromised their operations. Most officers, however, are apathetic, because thinking about these threats is just not part of their professional lives.

The one area of tradecraft which receives some DO attention, albeit slight, is the detection of surveillance. Case officers receive brief training in surveillance detection during their basic training. This training, however, is no more than an introduction to basic surveillance techniques, and in no way prepares officers for the real world.

When they are assigned overseas, however, case officers are expected to conduct surveillance detection routes prior to meetings with sources. In truth, the majority of case officers have insufficient knowledge to protect themselves from hostile surveillance, and because most DO stations have no detailed knowledge of the capabilities of the local counterintelligence service and police forces, case officers are not even aware of what they are up against. Certainly, a case officer facing a 20-man surveillance team, using multiple vehicles and an airplane would have to employ different tactics, than if he were facing a two-man team on a motorbike.

Scope of DO Intelligence Reporting

When I entered on duty with the DO in 1976, the CIA was described as the "President's Agency". This meant, I was told, that the DO's only customer was the President of the United States and his National Security Council. Somewhere over the last twenty odd years, however, this exclusive status changed. Now, the DO has numerous customers, including almost all government departments and agencies, as well as numerous congressional committees, who tend to task the DO according to their own desires, rather than according to the national interest.

Of course, Congress is responsible for oversight of the DO's activities to ensure that past abuses do not reoccur, and that its resources are being utilized properly. Congress must strive, however, to voluntarily limit its tasking of the DO to only those requirements that are vital to meet its responsibilities.

Not only does the DO now have an inappropriately large customer base, but its customers are voracious. Every year, they task the DO with an increasing number of requirements, the majority of which could and should be serviced by other agencies. These ever-increasing requests for non-vital, non-strategic intelligence, dilutes the DO's capabilities, and ensures that the DO will be unsuccessful in its efforts to focus on the most important intelligence issues in the future.

As an example, several years ago, the Director of CIA was visited by several leaders of a major U.S. industry. They convinced the Director that another country was perilously close to developing a new technology, which had both commercial and military applications, that would decimate their industry, and place the U.S. at a strategic disadvantage. After the meeting, Headquarters sent a cable to the field station in the country concerned, which was captioned "Urgent National Requirement". The cable explained the ostensible threat, and instructed

the station to initiate operations against this new target, which the station did forthwith.

The station sent a consistent flow of cables to Headquarters describing the progress it was making in its target analysis, and in identifying potential sources. At first, Headquarters responded quickly to the station's cables, but as time went on, Headquarters strangely fell silent on the topic. The station, in the absence of any contrary instructions, continued with the operation. Several months later, however, a Headquarters officer, who was visiting the station on another matter, informed the station that the Urgent National Requirement had been dropped. He explained that the industry officials discovered, mostly through open sources, that the U.S. industry was actually ahead of the country in question in developing the new technology.

This anecdote highlights the fact that the DO is tasked by a wide spectrum of customers to obtain information which can be obtained by other means, in this case, overt sources.

The impact of the increased scope of the DO's mission cannot be overstated. Instead of being the small, highly specialized organization it was meant to be, able to focus its clandestine skills on a relatively few, but vital requirements, while protecting itself and its operations, the DO has become a standard institution of the government - it has become "corporatized". By this, I mean the DO has become so concerned about pleasing and servicing its customers, that it tries to keep up with their continually growing appetite for information, rather than returning to its roots.

The dilution of the DO's mission helped create and reinforce a philosophy, and a bureaucratic structure, within the DO that is no longer tenable. Rather than focusing its operations on only those targets known to have access to valuable intelligence, the DO's philosophy has dictated the recruitment of as many sources as possible, via an international shotgun approach. This has resulted in a source base that is widespread, but shallow, and which frequently fails to provide policymakers with quality intelligence. Moreover, this philosophy created a single career-track structure within the DO, which demands and rewards quantity over quality.

In the DO, the majority of all staff case officers are recruiters. This is the only career track available for most officers, and this system has drastically limited promotions, which in turn, has created internal tensions, resulting in a large number of resignations among junior officers. It may come as a surprise, but the DO has no career track for

counterintelligence officers, agent handlers (officers who clandestinely meet and debrief recruited sources), or for specialists in operational security.

As recruiters, case officers are promoted by the number of sources they recruit, and overseas field stations are graded by the number of sources recruited by their case officers. This encourages and rewards case officers and stations alike to go after easier sources, rather than targets from the "hard target" countries, which include the remaining communist nations, Russia and the Balkan Republics, and the "rogue" states of the Middle East. Bureaucratically, the bottom line is that, at the end of the year, both case officers and stations will be graded and ranked, and if neither has anything to show for their annual efforts, no rewards will accrue.

Those who doubt the accuracy of the above statement need only look to recent history for proof. Senior policymakers have stated their displeasure with the DO's efforts, and have questioned why the DO lacks sources in many of the "hard target" nations. On one occasion, one senior policymaker went so far as to pointedly ask senior DO managers if the information provided by DO sources was qualitatively better than the information found in newspapers. There can be no greater indictment of a clandestine espionage service! Simply stated, if the DO is doing journalism, it isn't conducting espionage.

Moreover, because of recent budget and downsizing constraints on CIA, the DO was forced to find ways to cut its budget. It did so, in large measure, by terminating hundreds of sources that, heretofore, it had claimed to be its life's blood. This reveals not only that DO officers are forced to be prolific recruiters, it also emphasizes the fact that these sources were not the kind of high quality assets the DO was created to recruit.

The operational problems of the DO are serious, and must be addressed if the DO is to enter the next century as a viable and dynamic organization. Change within the DO alone, however, will not enable it to become the successful organization it must be. To optimize the DO's value, its customer base must be limited to the President, National Security Council, and the appropriate congressional oversight committees, and the requirements levied against it must only be those which cannot be obtained by any other means.

The Bureaucracy

Over the past several years, the DO has experienced a phenomenon that, heretofore, has never occurred - the resignation of a large number of

young officers, many of whom resigned while on their first tour overseas. This problem, virtually unheard of in the past, is so serious, that the CIA's Office of Inspector General initiated an investigation to discover the cause of the exodus.

The most important reason for these resignations is the DO's single career track, and the limitations this system places on promotions. In this era of budget cuts and downsizing, the DO is limited in the number of officers it can promote to higher rank. As a result, only a small percentage of officers are promoted each year. As one might imagine, because all officers are recruiters, the competition for promotion is fierce. The fact remains, however, that many officers, even those who have recruited sources, must wait years for a promotion. This, of course, has a negative impact on the officer corps, and leads to accusations that the system is unfair, and unresponsive.

Even at its best, the current system is ponderous, and open to abuse. If say twenty officers out of one hundred at the GS-11 level have recruited sources over the year, but only eight can be promoted, how does one decide which eight get the nod? If no hard targets are included in the mix, then is the decision made on simply the number of sources recruited, or on the quality of the intelligence they provide. If on quality, then how does one define quality? If quality is defined as the importance to the U.S. of the nation against which the source was recruited, then, in effect, officers assigned by the DO to less important countries, are unfairly disadvantaged through no fault of their own. If hard targets are a factor, then does one promote an officer for being lucky enough to be the station's "Duty Officer" when a Russian intelligence officer walks-in to the embassy and volunteers, over an officer who spent a year of professional effort to successfully recruit his source. And what happens to the officers who were just as, or maybe even more, professional than the twenty officers who recruited sources, but when the moment of truth came, the source turned them down. Recruitment, after all, like courtship, is not a one-way street.

One can also see how, in such a system, a certain amount of fraud and dishonesty can creep in. How many of the recruited sources are "paper-recruitments" - sources, which, on paper, are hyped to be much more valuable and impressive than is the actual case?

In an attempt to mitigate this problem, the DO launched a cash bonus program - money for good work. Many officers, however, regard this to be too mercenary, and they are not as much interested in financial remuneration, as they are in professional recognition.

This one-dimensional system leaves a lot to be desired. The current system does not recognize the varied strengths of its officers, or appreciate the fact that other duties are equally important to that of recruiting. Rather, the DO assumes that all of its officers will be good recruiters, which only serves to prevent other avenues to promotion, and goes a long way in alienating many officers by limiting their career advancement opportunities.

Aside from promotional limitations, however, there are other factors, which have adversely impacted on DO officers. In some cases, these factors might be more important to young case officers, than their restricted opportunities for career advancement. The following are just a few:

Case officers are frustrated by the criticism they hear of the DO, most of which they agree with, and with the apparent inability or unwillingness of the President and CIA senior managers to establish the leadership necessary to right the wrongs. I was overseas when the July 4, 1994 issue of U.S. News and World Report was published, the cover of which was emblazoned with an article entitled "The CIA's Darkest Secrets - An exclusive investigation of corruption and incompetence in America's spy service". A number of first and second tour officers read and discussed this article with me, stating their belief that virtually all the charges contained in the article were true. Sadly, two of them resigned not long after, and a third planned to resign after his next tour.

Case officers are also frustrated by the "reinvention of the wheel" which results from the steady and consistent change of CIA leadership. Every time a new Director of Central Intelligence (DCI) is appointed, he appoints a new chief for the DO, and the two men begin a long period of studying the DO's problems. After a considerable amount of time and effort, and many cables to the field stations explaining why certain policies were right, wrong, poorly timed, etc., a new policy is created and sent to the field, which for the most part is only a variation on a theme. Shortly thereafter, a new DCI is appointed, and the whole process begins anew.

As a result of all of the above, case officers lack pride. They are not proud of their jobs, their managers, or of their institution. They have no esprit de corps to fall back on when times are bad, because, sadly, there is no esprit de corps left. What DO case officers need more than anything else, is for their leaders to make the substantive, and systemic changes so sorely needed. These officers want to be good, and they want

to proud of their service. They also want and need for their leaders and their country to be proud of them.

Solutions: Limit DO Reporting

The President and the National Security Council (NSC), in partnership with the Congress, must retake control of the DO, and use it to obtain only that information which must be obtained through espionage. To accomplish this, the President and the NSC should demand more and better information from other government departments and agencies. These organizations must pull their own weight and attempt to answer many of the questions they currently levy on the DO. Each organization should also be required to demonstrate that all appropriate overt sources have been queried for answers, prior to submitting a request for a specific question to be nominated as a national security requirement.

The NSC should then initiate a policy of sifting through all questions nominated to be national security requirements, to ensure that only vital and strategic requirements, and only those worth the risk of exposure, are levied on the DO.

Operations - Provide Better Cover

Before any operations abroad can succeed, case officers must have cover good enough to hide their true affiliation, and their operations. Therefore, the DO must discontinue assigning most of its case officers to U.S. Embassies abroad, although there will always be a need to have some case officers assigned undercover in embassies, so they can spot and assess official targets. Our embassies are incompatible with cover, because they are permeated with Foreign Service Nationals, many of which work against our interests, and the embassies are a natural point of focus for local counterintelligence services. In effect, the U.S. Government has announced to the local service that all of our personnel, including our intelligence officers, are located within the embassy. This provides the local service with an immediate advantage over the DO's case officers - counterintelligence officers know where they are, and can spend their resources investigating a single location.

To counter this threat, DO case officers must be assigned to non-official cover positions, mostly in commercial entities. When our case officers are hidden among thousands of U.S. businessmen, it will be almost impossible for local counterintelligence officers to uncover them, and hence, their personal and operational security will be greatly enhanced. The DO is already working on this type of cover, but more needs to be done, and on a greater scale.

Provide Case Officers with the Appropriate Skills

In espionage, two factors are constant. Intelligence officers recruit foreign nationals who can provide classified information on their government's plans and intentions, and the counterintelligence services of those countries try to thwart these operations. The DO recognizes these facts, but only as it concerns operations in "hard target" countries. It is time for the DO to recognize that its operations in the rest of the world also face counterintelligence threats.

In this regard, the DO must recognize that its officers are only unique if they have the talent and skills to operate clandestinely. If not, they are no different than officers from the other government departments, or journalists, who, in order to be discreet, try to protect their contacts. Therefore, it is essential that all DO officers be well trained in the disciplines of cover, counterintelligence, and operational security. Rather than a three-day bloc of instruction, this training should be extensive, and provide the foundation on which all officers build their careers. When the nation looks to the DO to operate clandestinely, the DO must be able to respond with expertise and professionalism.

Bureaucracy - Reorganization

The recruitment of human sources is the primary function of the DO. In this regard, it should be noted that there are a small number of officers who are natural born recruiters. They can recruit sources anywhere, anytime. These officers are invaluable to the DO's mission, and should be recognized and rewarded for their unique and valuable skills. The DO should identify those officers who have the innate ability, and the desire to be recruiters, and form them into a special corps. The fighter pilots of the CIA if you will, first among equals. These officers would be used selectively to recruit targets that have painstakingly been identified, investigated, and developed by their colleagues. This is roughly how the Mossad (Israeli Intelligence) operates, to great effect. More career tracks should be opened to DO officers. Given the vital importance of counterintelligence, operational security, and agent handling, it simply does not make sense for the DO to expect and insist that all of its officers be recruiters. The skills required for counter-intelligence, operational security, and agent handling, vary widely. The DO should identify those officers who have the interest and skill to excel in these disciplines, and provide them with career tracks that recognize and reward their efforts.

Because all case officers are hired as generalist recruiters, the DO believes that all of its officers should be able to recruit anywhere in the

world, without a high degree of language ability, or an in-depth knowledge of the country and region to which they are assigned. As a result, DO officers only spend two to three years on assignment, before being reassigned to another country, frequently a country with a different language and culture. DO officers, therefore, do not have sufficient language skills to operate effectively, nor do they have the degree of area familiarization required for them to operate skillfully and securely. To remedy this situation, increased language and cultural skills are sorely needed, particularly for officers going to areas less familiar to Americans, such as Asia, and the Middle East.

Prior to one of my assignments, I was given only five months of language training, yet I was expected to recruit new sources, and handle recruited sources, in that language. It does not take much imagination to understand that if an officer cannot adequately converse with a target, he or she will be unlikely to obtain the target's trust and confidence. And, without both the language ability, and an in-depth knowledge of the country and region to which the case officer is assigned, he or she will be relegated to the position of student, rather than equal, when dealing with a target, or a recruited source.

This is problematic when one considers that, in some cultures in Asia and the Middle East, being seen as equal, or even superior, is essential to gaining the admiration and respect of targets, and hence in recruiting and handling them. To be anything less in the eyes of such a target, or recruited source, is an open invitation to failure.

Therefore, DO officers should be encouraged and rewarded for specializing in at least one language, and to obtain an in-depth knowledge of a given country or region. Officers should be assigned to a specific region, and their overseas tours should be within that region.

As an example, a China specialist, should be proficient in Mandarin Chinese, and should spend his or her career moving throughout the region, with assignments to the People's Republic of China (PRC), Hong Kong, Taiwan, and perhaps Singapore, which is ethnically seventy five percent Chinese. In this way, the officer's language ability would constantly be reinforced, and improve with use, and he or she would develop an intimate knowledge of the personalities, politics, economics, and culture, of the region. This expertise would enable the officer to converse with targets on an equal, or superior level, and, no less important, to understand the significance of what the target says.

Many foreign intelligence and diplomatic services require their officers to specialize in a given area and language because this system

works. During my career, I found that my counterparts from the Soviet Union, the PRC, or from countries such as France and Singapore, were much better linguists, and much more knowledgeable than me or my colleagues, about the countries to which they were assigned.

As an example of how DO officers compare with some of their foreign counterparts, most officers preparing for a tour in the PRC receive approximately two years of language training, one of the DO's longest training courses. Graded on a five point system - 1 being a beginner, and 5 being a native speaker - students usually graduate from this course with a rough 3 level. At this level, a student has the basic ability to converse socially, and has the infrastructure to reach a higher level of communication with work and use. Generally speaking, these officers receive no instruction in the culture, history, or politics of the PRC prior to being assigned in-country. After spending a two-year tour in China, many of these officers will be reassigned to countries outside of the region, thereby losing much of their language ability, as well as the substantive knowledge they obtained.

By contrast, one of my contacts from the PRC told me that before he was sent on his first assignment, he received French language training for five years in Beijing. He was then assigned to West Africa (former French Africa), where he used his language skills for another five years, after which he was assigned to Paris. He believed he would remain in Paris for approximately five years, and expected to return to West Africa after his tour in Paris ended.

Conclusion

Because of the myriad dangers and forces arrayed against the United States, it is essential for our country to have a capable and dynamic DO. Billions of dollars and the safety of our citizens at home and abroad are at stake. But, in order for the DO to perform its mission effectively, change is necessary. Recruitment of human sources, the DO's main responsibility, must continue, but the DO must concentrate its efforts on only those targets, which have access to vital and strategic intelligence. The DO must also ensure that its officers have viable cover, and are well trained in the disciplines of counterintelligence, and operational security, without which its recruitment efforts will falter.

These changes will not come easily, and will require the active participation of senior DO officials, the President and the NSC, as well as Congress, in a bi-partisan effort to reform the CIA and DO, in order to make it the highly specialized foreign policy tool it was intended to be.

No degree of reform within the DO, however, will succeed unless

the scope of DO reporting is limited to only that information which must be acquired through espionage. This will enable the DO to focus its efforts on the truly "hard targets", instead of having its efforts diluted to the point of journalism.

In addition, reform must include the willing and enthusiastic participation of the DO's men and women. They must be convinced that their leaders regard them as talented, and essential members of the team, and they must be provided with the opportunities for career advancement that, at present, do not exist. Therefore, new career tracks must be created for them. Keeping in mind that all case officers are not natural recruiters, officers must have the option of varied career paths, such as counterintelligence, operational security, and agent handling. These new career tracks are not only important to DO personnel, but are vital if the DO's operations are to be secure and successful.

Reform, however, will not be accomplished quickly. Rather, it will take a long time to reorient, and restructure the DO's method of operation, as well as its personnel. This will also require substantial funding, which should be seen as a necessary investment in national security. The reward will be a new, and dynamic DO, which will provide the policymakers with the key, strategic intelligence they require to guide our foreign policy into the future.

PREPARED STATEMENT OF NICHOLAS EFTIMIADES, AUTHOR OF *CHINESE INTELLIGENCE OPERATIONS*

Mr Chairman,

I thank you for the opportunity to speak before this Committee today. I'd like to take a brief moment to emphasize that I speak today as an author and private citizen; not as a representative of the Department of Defense or the U.S. government.

The operational methods of the China's intelligence services are nothing new to espionage. Those methods are, however, uniquely Chinese in their application. To collect technology and trade related information, China's premier intelligence services -- the Ministry of State Security (MSS) and the People's Liberation Army/General Staff Department/Second Department (also known as the Military Intelligence Department) -- co-opt vast numbers of Chinese citizens living or traveling overseas. The MSS also runs aggressive surveillance and recruitment programs against visiting foreign businessmen, scholars, government officials, and scientists.

Senior U.S. counterintelligence officials compare China's methods to classical Russian espionage techniques, which used fewer people but gathered more information per person. The Chinese approach poses many problems for U.S. law enforcement efforts, according to FBI counterintelligence chief Harry Godfrey III: "For prosecutive purposes, you are looking at an individual collecting one small part one time, and you don't have the quality of case that our country will take to prosecute as far as espionage."

Foreign Operations

Most of China's clandestine economic espionage activities are not sophisticated operations, but their numbers compensate for this weakness. In the U.S., those activities focus on the theft of American technology. For example, In the early 1990s the PRC's clandestine collection operations in the United States expanded to the point where approximately 50 percent of the nine hundred technology transfer cases investigated annually on the West Coast involved the Chinese. This figure is interesting when examined in the context of the list compiled by the Justice Department's Export Control Enforcement Unit, Internal Security Section, and published as Significant Export Control Cases from January 1981 to May 1992.

Statistical analysis of the Department of Justice list indicates that only 6 percent of 272 significant cases involved China, and that 62.5

percent of those cases occurred on the West Coast. In addition, 13.4 percent of the incidents listed in Department of Commerce Export Enforcement Cases: Closed January 1, 1986, to March 31, 1993, involved the PRC. Much of China's espionage efforts in industrialized nations is focused on mid-level technology, that may or may not be cleared for export. The focus of this economic espionage on mid-level technology is because China's technological industrial infrastructure is still 10-15 years behind the United States.

Illegal acquisition of such items draws less interest from U.S. law enforcement agencies and judicial organs (i.e., state and federal prosecutors and the courts) than does the theft of state-of-the-art technology. For that reason the PRC's technology-related intelligence collection operations have gone relatively unimpeded.

Computer-assisted analysis of China's exposed technology-related economic espionage activities in the United States reveals three basic operational patterns. First, co-optees are recruited in China and asked to acquire the targeted technologies while they travel abroad. Second, American companies with access to the desired level of technology are purchased outright by Chinese state-run firms. In intelligence circles this is considered a bold or aggressive operation. Third and most commonly, high-technology equipment is purchased by recruited agents running front companies. China's most productive method of legally acquiring foreign technology is to send scientists overseas on scholarly exchange programs.

Each year several thousand Chinese citizens travel to the U.S. trade missions, scientific cooperation programs, and the like. It is a normal, "open" intelligence procedure to debrief the returning delegates to determine whether useful information was acquired by simple observation. However, the MSS and military intelligence services further exploit these opportunities by co-opting a number of these travelers to carry out specific operational activities.

The operational differences between professional intelligence officers and co-opted individuals are often noticeable. The intelligence officer generally has less technical knowledge about the subject matter involved in the operation, while the co-optee usually has no expertise in collecting information clandestinely. For example, at a trade show in Paris, French military investigators observed members of a Chinese scientific delegation discreetly dipping their ties in a photo processing solution made by the German firm Agfa.

The goal of this clumsy act of espionage was presumably to obtain specimens of the solution for later analysis. Technology-related

clandestine intelligence activities are by no means limited to scientific and trade delegations. The PRC has attempted to purchase U.S. firms with access to high technology not authorized for release to foreign countries. In February 1990 the United States, citing national security concerns, ordered the China National Aero-Technology Import & Export Corp. (CATIC) to divest itself of Mamco Manufacturing Inc., a Seattle aircraft parts manufacturer.

The Bush administration said publicly that CATIC had a "checkered history" and had sought technology that would provide the Chinese People's Liberation Army's Air Force with in-flight refueling capabilities. More disturbing to administration officials was the belief that CATIC used Mamco as a front to penetrate other, more promising areas of restricted technology.

The purchase of a large American company is a rare operation compared to the more frequent economic espionage activities of the MSS, which generally procures technology through more subtle and clandestine means. It appears that the most effective means of stealing foreign technology involves the use of recruited agents in Hong Kong. I should emphasize that not enough time has elapsed since the return of Hong Kong to the PRC to identify any change in operational patterns.

Examination of several public cases of attempted (and successful) thefts of high technology reveals a unique pattern of operation. The recruited agent establishes a front company in Hong Kong. The company may in fact carry on legitimate trading activities in addition to illegally purchasing and shipping technology. The agent approaches several U.S. firms and tries to purchase restricted high-tech equipment--either in person at trade shows, over the phone, or by fax Sub-sources within the target country can be used to facilitate purchasing and shipping transactions.

Domestic Operations

At first glance, the intelligence and security environment in the PRC may appear to be relatively benign. The only categories of people who routinely report surveillance or other forms of harassment are dissidents and foreign journalists. The average business, tourist, or academic, visiting China does not immediately notice surveillance or overt intelligence collection activities. However, an internal security structure that collects information is woven into the fabric of Chinese society as well as into its economic, cultural, and political infrastructure.

Chinese intelligence services can count on state ministries, people's friendship societies, academic institutions, and the military-industrial

complex to support activities such as agent recruitment and information collection as well as to provide cover jobs to their operatives. Many PRC domestic intelligence activities are directed against foreign businessman or technical experts. The data elicited from unsuspecting persons or collected by technical surveillance means is used by Chinese state run or private enterprises.

In China, intelligence operations against foreign nationals include targets such as businessmen, government officials, academics, journalists. The MSS recruits these people to conduct espionage against their home government, to influence events overseas on behalf of the PRC, or to provide business intelligence and restricted technology.

The MSS and China's Military Intelligence Department (MID) invite foreign scholars and technical experts to lecture or attend conferences in the PRC under the guise of research associations or universities. All expenses for the visiting lecturer and his or her family frequently are paid for by the intelligence services. The visiting specialist is subjected to a demanding itinerary of lectures, meetings, travel, and social engagements. The purpose of this rigorous schedule is to wear down the prospective recruit's physical and mental stamina. The visitor is encouraged to partake of alcohol as much as circumstances permit. The subject is then more approachable concerning personal or confidential matters.

Academics, businessman, and other subject-matter experts are potentially lucrative targets for the PRC intelligence services for two reasons: (1) they possess unique insights in fields of interest to the MSS or MID, and (2) they have access to policymakers and other potential recruitment targets. In the first scenario, less subtlety is required to solicit information because the individual came to China expecting to provide details on a specific subject. The second scenario necessitates a more discreet approach. Another intelligence objective achieved by hosting foreign scholars is to persuade and co-opt those who are in positions to influence policymakers or businessman in their home countries.

The MSS appears to be far more comfortable recruiting persons of Chinese descent as opposed to non-Chinese foreign nationals. But one must consider that Beijing expects ethnically Chinese foreign nationals to have some loyalty to China. As a result, espionage recruitment techniques used against such persons in some ways resemble those used against Chinese nationals; the primary motivating factors being ethnic loyalty, implied threats of reprisals against PRC national relatives, and money gain.

Technical Surveillance

A key aspect of the PRC's internal collection network against foreign targets is the aggressive use of technical surveillance measures. Many of the prominent hotels that cater to foreigners are equipped for the technical surveillance of guests and visitors. Technical surveillance of foreigners in these and other Chinese hotels is carried out by the MSS's Technical Operations Department.

In May 1989 Chinese student dissident Wuer Kaixi was recorded on videotape as he ate lunch with foreign journalists in the Beijing Hotel. The tape was made by the hotel's static surveillance cameras, located in the ceiling of the dining room. Other prominent Beijing hotels that are known to monitor the activities of their clientele are the Palace Hotel, the Great Wall Hotel, and the Xiang Shan Hotel. In addition, the MPS owns the Kunlun Hotel and probably monitors its guests. And according to Chinese prostitutes who frequent the Jianguo Hotel, the guest rooms used by foreign businessmen there also contain microphones.

The Palace Hotel is owned in part by the PLA's General Staff Department. One of the American contractors for the Xiang Shan Hotel had a series of verbal battles with PRC officials as it was being built. The Chinese demanded that additional wires be installed in each room. The purpose of the wires was to tie in microphones.

The video and audio surveillance of foreigners in China is the responsibility of the MSS. The monitoring of international mail and telecommunications involving Chinese nationals is handled by the Ministry of Post and Telecommunications.

Conclusion

Western policy, intelligence, and law enforcement agencies must adjust the focus of their collection and counterintelligence operations if they are to contend effectively with the PRC's economic espionage activities. At the policy level an increased emphasis on protecting commercial intelligence and monitoring illegal technology transfer issues is needed. In the United States, the notion of government helping private industry to protect itself from foreign intelligence activity is controversial. Providing industry with foreign high technology and economic intelligence, as practiced in the PRC, is not a policy option in the United States. For that reason, presidential administrations must supply strong leadership and thoughtful guidance to private industry on the issue of safeguarding sensitive advanced technology and corporate trade secrets.

Washington must establish the type of relationship with business that promotes the mutual development of policy guidelines for protecting sensitive technology. Such guidelines will be difficult to develop and implement due to the necessity of maintaining the domestic free flow of ideas. The legislative and judicial branches of government must also be made aware of the seriousness of illegal high-technology transfers and their potential impact on U.S. national security.

At the working level, intelligence and law enforcement agencies must redirect their operational focus and allocate the appropriate resources to specialized area studies, analyses of PRC intelligence tradecraft, and linguistic capabilities. The shifting of U.S. counter-intelligence concerns is likely to be a long, slow process due to fiscal restraints, competing agency interests, and bureaucratic inertia. Congressional oversight of this process may be wise, because intelligence bureaucracies tend to be self-perpetuating and therefore resistant to change.

Another impediment to effective action against Chinese economic espionage is the state of relations with Beijing established by the Bush administration and continuing to this day. Privately, FBI agents say that "in the scheme of things these days, it seems to make very little difference to Washington whether the Chinese are spying or not . . . it's almost an annoyance when an actual violation of law surfaces."

Given the institutional problems involved in altering the focus of U.S. counterintelligence efforts, the MSS will probably continue to penetrate and exploit the United States' and other Western nations' political, academic, industrial, and technological institutions. As the MSS expands its operations globally, its methods can be expected to increase in sophistication as well.

○

ISBN 0-16-057337-8