S. Hrg. 105–614

CYBER ATTACK: IS THE NATION AT RISK?

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

JUNE 24, 1998

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

50–293 cc WASHINGTON : 1998

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-057471-4

COMMITTEE ON GOVERNMENTAL AFFAIRS

FRED THOMPSON, Tennessee, *Chairman*

WILLIAM V. ROTH, JR., Delaware	JOHN GLENN, Ohio
TED STEVENS, Alaska	CARL LEVIN, Michigan
SUSAN M. COLLINS, Maine	JOSEPH I. LIEBERMAN, Connecticut
SAM BROWNBACK, Kansas	DANIEL K. AKAKA, Hawaii
PETE V. DOMENICI, New Mexico	RICHARD J. DURBIN, Illinois
THAD COCHRAN, Mississippi	ROBERT G. TORRICELLI, New Jersey
DON NICKLES, Oklahoma	
ARLEN SPECTER, Pennsylvania	MAX CLELAND, Georgia

HANNAH S. SISTARE, *Staff Director and Counsel*
ELLEN B. BROWN, *Counsel*
JOHN P. PEDE, *Professional Staff Member*
WILLIAM C. GREENWALT, *Professional Staff Member*
JOHN H. COBB, *Investigative Counsel*
MARGARET A. HICKEY, *Investigative Counsel*
LEONARD WEISS, *Minority Staff Director*
DEBORAH COHEN LEHRICH, *Minority Assistant Counsel*
LYNN L. BAKER, *Chief Clerk*

CONTENTS

CYBER ATTACK: IS THE NATION AT RISK?

WEDNESDAY, JUNE 24, 1998

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Fred Thompson, Chairman of the Committee, presiding.

Present: Senators Thompson and Lieberman.

OPENING STATEMENT OF CHAIRMAN THOMPSON

Chairman THOMPSON. The Committee will come to order, please. I welcome our witnesses this morning.

The Governmental Affairs Committee today is holding its second in a series of hearings on the security of Federal computer systems. Anyone who thinks that that is a dull subject will, I think, quickly be disabused of that notion. In fact, I think they probably already have if they have listened to some of the hearings that we and other committees have already had.

Today's hearing will focus on the intelligence community's assessment of the threats to our Nation's information systems. During our hearing last month, we heard that the foundation of our Nation's information infrastructure is riddled with security vulnerabilities and flaws.

The L0pht hacker think tank, which testified at our earlier hearing, stated that they "could very trivially make the Internet unusable for the entire Nation." This has serious implications when considering how dependent our society has become on the Internet. L0pht also testified that, given enough resources, a small group of skilled hackers could wreak havoc on our country—ranging from shutting down communications systems and utilities to causing unstable financial markets.

Dr. Neumann, a renowned computer security expert who also testified, agreed with this, stating that "massive coordinated attacks on our infrastructure are possible; however, it may take a Chernobyl-scale event to raise awareness levels adequately, perhaps bringing several of the national infrastructures to their knees simultaneously."

We cannot wait for such an electronic Pearl Harbor or Oklahoma City to recognize that there is a serious problem. At risk are the systems that control national security, air traffic, finances, power, and communications. To date, the mainstream media has focused on unsophisticated hacking of governmental systems. That does not accurately represent the seriousness of the threat.

We often read about the hackers that have been caught, but what about the sophisticated hackers who are not detected, who are not caught? What gives me great concern is that we simply do not know what we do not know. According to a 1996 estimate by the Defense Information System Agency, as many as 250,000 attacks occurred on defense systems in 1995. How many of these were actually detected? How many of the perpetrators were caught? How many viruses were left behind? How much critical data was compromised? Unfortunately, we simply cannot answer those questions.

Of course, this is not the major problem. We see that we increasingly have concerns about being targeted by other nations and other groups. As the American way of life becomes increasingly dependent on computer systems and the uninterrupted flow of information, the use of information technologies as a tool of warfare and terror become increasingly likely. Instead of confronting us head to head on the traditional battlefield where they would undoubtedly lose, adversaries will confront the United States at its point of least resistance—and that is our information infrastructure. Cyberspace is the battlefield of tomorrow.

This is well understood by our potential adversaries, whether it be other nations or terrorists, drug cartels, or organized crime groups. They can reach deep into our homeland from the sanctity of theirs. This is not just a theory. We know for a fact that terrorists and organized crime groups are developing information warfare systems. A recent *Newsweek* article claims that there are about ten countries, in addition to China and Russia, with information warfare programs. Among these countries are Libya, Iraq, and Iran, and, of course, they are not friends of the United States, and all of them sponsor anti-American terrorists.

I do not believe that this is a futuristic threat, as some portray it. The threat is real, it is serious, and it is here today. Cyber weapons are being developed, countries are incorporating strategies into their doctrine, our computer systems are being probed to identify vulnerabilities, and our defenses are weak.

I believe that protecting our Nation against cyber attack represents one of the greatest challenges that we have faced as a country. We must act now to develop the policies, plans, programs, and strategies to deter this threat.

Today, we will hear from the leaders of our intelligence community, the Hon. George Tenet, Director of the Central Intelligence Agency, and Lieutenant General Ken Minihan, Director of the National Security Agency. Mr. Tenet will provide an assessment on the threats to our information infrastructure and what is being done to address these threats. General Minihan will testify on the findings from the military exercise called "Eligible Receiver," which identified serious vulnerabilities of our Nation's computer system.

Senator Lieberman.

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. Thank you, Mr. Chairman. Once again, let me thank you for holding this hearing and let me join you in welcoming Mr. Tenet and General Minihan.

Mr. Chairman, I am struck, as I was at our May hearing on computer security, by the enormity of the problem that we are discussing today. The scope of the threat that we are facing, which is to say the ability of foreign governments or non-governmental hostile groups, such as terrorists, to effectively shut down our economy and to hamper our military's ability to operate effectively is obviously worrisome and profoundly unsettling.

We are all accustomed to thinking of computers as a great benefit, and they usually are. They give us instant access to all sorts of information at any time of day or night. They make our trains and planes run effectively and smoothly. They operate our power systems. They have made it so that I, for instance, am able through E-mail to stay as closely in touch with one of my children who is in school in England as my parents were able to with me when I was in college just a couple of towns away from them—and may I add, I do so at less cost than they did.

Computers, in short, particularly the interconnection of computer networks through the Internet, have revolutionized our lives, almost always for the better. But as this Committee's examination of this problem is showing, with the computer information age revolution has come a new kind of dependency and, therefore, a new form of vulnerability. Unfortunately, we have been slower to appreciate the risks of the computer revolution than we have been to take advantage of its benefits.

As our witnesses will explain to us today, our critical infrastructures—banking, financial, communications, transportation, security—are all dependent on computer systems and, therefore, are vulnerable. And each of these computer systems can be hacked into and disrupted.

If we were dealing only with a group of young hackers, that would be troubling enough. But as we will hear today, we face much more sophisticated and ominous and hostile threats than a bunch of teenagers engaged in a New Age rite of passage. A number of terrorists groups and nations are adding cyber warfare weapons to their arsenals. They are developing the ability to hack into computer systems, and once in them, to disrupt or even shut down parts of our economy to affect significantly our military's ability to do its job.

In fact, as one of our witnesses may indicate today, some experts predict that this type of information warfare can be as effective at immobilizing our defenses as some of the conventional weapons or weapons of mass destruction that we are focused on.

This, naturally, worries all of us. It should worry all of us. Of course, it should also propel us to work together to build a system of defenses to this new high-tech threat to our national security.

So, Mr. Chairman, I truly appreciate your holding these hearings. They are critically important. I thank you for illuminating what might be described as the down side of our entrance into cyberspace and the information age. I look forward to hearing from our distinguished witnesses today, and most importantly, I look forward to working with them and you and others in the Congress to develop methods for better protecting ourselves from the threat of IW, of information warfare. Thank you.

Chairman THOMPSON. Thank you very much.

Mr. Tenet.

TESTIMONY OF THE HON. GEORGE J. TENET, DIRECTOR OF CENTRAL INTELLIGENCE

Mr. TENET. Thank you, Mr. Chairman. Just like the proliferation of weapons of mass destruction, international terrorism, and drug trafficking, information warfare has the potential to deal a crippling blow to our national security if we do not take strong measures to counter it.

Consider, for example, the *Washington Post* report early this year that 11 U.S. military systems were subjected to an electronic assault. The perpetrators were not initially known because they hid their tracks by routing their attack through the United Arab Emirates computer systems. While no classified systems were penetrated and no classified records were accessed, logistics, administration, and accounting systems were accessed. These systems are the central core of data necessary to manage our military forces and deploy them to the field. In the end, we found two young hackers from California had perpetrated the attacks via the United Arab Emirates under the direction of a teenage hacker from Israel.

This should not surprise us. As you mentioned, Mr. Chairman, a recent DoD study said that DoD systems were attacked a quarter of a million times in 1995. As a test, the Defense Department organization that same year conducted 38,000 attacks of their own. They were successful 65 percent of the time, and 63 percent of the attacks went completely undetected.

We have spent years making systems interoperable, easy to access, and easy to use, yet we still rely on the same methods of security that we did when data systems consisted of large mainframe computers housed in closed rooms with limited physical access. By doing so, we are building an information infrastructure, the most complex the world has ever known, on a very insecure foundation. We have ignored the need to build trust into our own systems. Simply hoping that someday, we can add the needed security before it is too late is not a strategy.

In this hearing today, Mr. Chairman, I hope to leave you with three key points. First, I want you to take away an appreciation for the growing seriousness and significance of the emerging threat to our information systems.

Second, I want to emphasize the need to evaluate the threat from the perspective of both State and non-State actors. Proliferation of malicious capabilities exist at every level.

And finally, I want to provide you with an appreciation for what the intelligence community is doing to combat the problem. On this last point, let me assure you that our engagement in infrastructure protection extends not just to efforts within the intelligence community, but to participation with all other stakeholders in our Nation's infrastructure systems, across government agencies, in academia and the private sector.

As this Committee well understands, we have staked our way of life on the use of information. We rely more and more on computer networks for the flow of essential information. Like electricity, we now take information infrastructures for granted. Reliability breeds dependence and dependence breeds vulnerabilities. Today, as a re-

sult of the dramatic growth of and dependency on new information technologies, our infrastructures have become increasingly automated and interlinked.

Disruptions in information based on technologies can range from being a serious nuisance, as we saw just weeks ago when the loss of a single satellite caused a nationwide halt in electronic pager systems, to the potentially disastrous. Consider what such a disruption would have caused to Operation Desert Storm, where our information systems had to accommodate a communications volume of 100,000 electronic messages and 700,000 telephone calls a day. Seven years later, those figures would be far greater and our reliance on computers is much greater, as well.

It is in this context that we must appreciate that future enemies, whether nations, groups, or individuals, may seek to harm us in nontraditional ways. Nontraditional attacks against our information infrastructures could significantly harm both our military power and our economy.

Who would consider attacking our Nation's computer systems? Yesterday, you received a classified briefing answering this question in some detail, Mr. Chairman. I can tell you in this forum that potential attackers range from national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers, and disgruntled or disloyal insiders. Each of these adversaries is motivated by different objectives and constrained by different levels of resources, technical expertise, access to a target, and risk tolerance.

Why would we be attacked? There are plenty of incentives—trillions of dollars in financial transactions in commerce moving over a medium with minimal protection and sporadic law enforcement, increasing quantities of intellectual property residing on network systems, and the opportunity to disrupt military effectiveness and public safety with the elements of surprise and anonymity. The stakes are enormous. Protecting our critical information infrastructure is an issue that we should all be deeply troubled about.

As I recently testified before the Senate Intelligence Committee in January, we have identified several countries that have government-sponsored information warfare programs. Foreign nations have begun to include information warfare in their military doctrine as well as their war college curricula with respect to both defensive and offensive applications. It is clear that nations developing these programs recognize the value of attacking a country's computer systems, both on the battlefield and in the civilian arena.

The magnitude of the threat from various forms of intrusion, tampering, and delivery of malicious code is extraordinary. We know with specificity of several nations that are working on developing an information warfare capability. In light of the sophistication of many other countries in programming and Internet usage, the threat has to be viewed as a factor requiring considerable attention by every agency of government.

Many of the countries whose information warfare efforts we follow realize that in a conventional military confrontation against the United States, they cannot prevail. These countries recognize that cyber attacks, possibly launched from outside the United States against civilian computer systems in the United States rep-

resent the kind of asymmetric option they will need to level the playing field during an armed crisis against the United States.

Just as foreign governments and the military services have long emphasized the need to disrupt the flow of information in combat situations, they now stress the power of information warfare when targeted against civilian information infrastructures. The three following statements, all from high-level foreign defense or military officials, illustrate the power and the import of information warfare in the decades ahead.

For example, in an interview late last year, a senior Russian official commented that an attack against a national target, such as transportation or electrical power distribution, would, "by virtue of its catastrophic consequences, completely overlap with the use of weapons of mass destruction."

An article in China's People Liberation Daily stated that, "An adversary wishing to destroy the United States only has to mess up the computer systems of its banks by high-tech means. This would disrupt and destroy the U.S. economy. If we overlook this point and simply rely on the building of a costly standing army, it is just as good as building a contemporary Maginot Line."

A defense publication from yet a third country stated that "information warfare will be the most vital component of future wars and disputes." The author predicted bloodless conflict since, "information warfare alone may decide the outcome."

As these anecdotes clearly demonstrate, the battle space of the information age will surely extend toward domestic infrastructure. Our electric power grids and our telecommunications networks will be targets of the first order. An adversary capable of implanting the right virus or accessing the right terminal can cause massive damage.

Information warfare is not just about offensive capability, however, but about defensive readiness, as well. This fact has not been lost on others. Many nations, several of which are potential adversaries, are reviewing their own growing dependence on information systems, both for military and civil activities. They are searching out their vulnerabilities and developing approaches to protect themselves. We must do the same. If not, we could soon find ourselves at a significant disadvantage in addressing what may be the key security challenge of the next decade and beyond.

Next, Mr. Chairman, I want to examine the degree to which this threat has proliferated beyond traditional nation states to become the potential weapon of choice for less structured adversaries. Terrorists and non-State actors are beginning to recognize that information warfare offers them new, lost-cost, and easily-hidden tools to support their causes. They, too, will see the United States as a potentially lucrative target. These people will be very difficult for the United States to trace in cyberspace.

Terrorists, while unlikely to mount an attack on the same scale as a nation, can still do considerable harm. What is worse, the technology of hacking has advanced to the point that many of the tools which required in-depth knowledge a few years ago have become automated and more user friendly. It may even be possible for terrorists to use amateur hackers as their unwitting accomplices in a cyber attack. Cyber attacks offer terrorists the possibil-

ity of greater security and operational flexibility. Theoretically, they can launch a computer assault from almost anywhere in the world without directly exposing the attacker to physical harm.

Terrorists are not bound by traditional norms of political behavior between states. While a foreign state may hesitate to launch a cyber attack against the United States due to fear of retaliation or negative political consequences, terrorists often seek the attention and the increasing fear that would be generated by such a cyber attack.

Established terrorist groups are likely to view attacks against information systems as a means of striking at government, commercial, and industrial targets with little risk of being caught. Global proliferation of computer technology and the open availability of computer tools that can be used to attack other computers make it possible for terrorist groups to develop this capability without great difficulty.

Terrorists and extremists already are using the Internet and even their own web pages to communicate, raise funds, recruit, and gather intelligence. They also will use it to launch attacks against their adversaries. They may even launch attacks remotely from countries where their actions are not illegal or with whom we have no extradition agreements. Let me give you a few examples of what I am talking about.

The group calling themselves the Internet Black Tigers took responsibility for attacks last August on the E-mail systems of Sri Lankan diplomatic posts around the world, including those in the United States. Italian sympathizers of the Mexican Zapatista rebels crashed web pages belonging to Mexican financial institutions. While such attacks did not result in damage to the targets, they were portrayed as successful by the terrorists and used to generate propaganda and rally supporters.

Mr. Chairman, as terrorists and other adversaries well know, our society is based on the free flow of information. That concept is clearly embodied in the Constitution. It forms the foundation of our freedoms and of our productivity. Consequently, our systems are built to facilitate access and openness and they must remain so within the reasonable bounds of security. It is just that openness, however, that makes our system so vulnerable.

So how will we detect an attack in this world of vast interconnectivity? It will not be easy. In the first place, those who would attack us generally are tough intelligence targets. Second, they will use cheap, easily available technology and techniques. Patterns will be difficult to spot.

Furthermore, intrusion detection technology is still in its infancy and the systems we will need to observe are very diverse. When attacks are detected, the source of the attack will be disguised. Moreover, after trouble is detected, it takes time for an analyst to determine whether the problem took hold by accident or by design. Unless we have intelligence indications dealing with someone's intention to attack, such as through a human source, tactical warning will be very, very difficult to attain.

However, by combining the efforts of government and industry, we will be able to pool our strengths and share the necessary information to allow a reasonable defense. By sharing the research and

development burden between public and private sectors, we each will be better able to take advantage of the other's expertise. This is one of the advantages of connectivity.

In my written statement, Mr. Chairman, I have described numerous initiatives and working groups in which the intelligence community is involved to better handle the information warfare threat. These range from our national intelligence estimate devoted to this topic to establishing new units within the community to focus on this problem full time. Further, as you can see from the written statement, we have made great strides in our cooperative efforts with the Departments of Defense and Justice to overcome cross-agency challenges that the information age creates.

Since those efforts are laid out in the written statement, I would like to return to a theme raised earlier in my remarks and tell you more about what I mean. Having created our information systems on a foundation that lacks adequate security, we have to focus on building trust into our systems. What do I mean?

It is more than just security. Security is concerned with locks and fences and guards. Trust is the belief that the security works. Security involves more than just encryption. It is also about authentication and digital signatures and data integrity. Trust is about key management, digital certificates, and policies, such as what your privileges are and what you are authorized to do with your digital signatures. Making our systems secure and trustworthy, while not an intelligence community issue per se, is the ultimate solution to the threat of information warfare.

I know, Mr. Chairman, that you plan to have a hearing later on about how we do the protection side of the business. I would say to you that it is very clear that we have shared vulnerabilities between the private sector and the government and what we do not have today is a system of trust that ensures both the privacy of the information we seek to pass and the ability to protect that information.

We have had an enormous debate in this country about encryption. Encryption is not the issue. The issue is, is there a system in place that allows us to authenticate you as the user? Is there a system in place that allows us to understand whether you have the responsibility or the right to transfer the information that you have transferred? Is there a system in place that allows you to verify that the data that you have transferred has not been manipulated?

There is no such system in place and the private sector and the government have a responsibility to work towards this. If such a system was in place, if we could protect the integrity of the data and its authentication, we would deny our adversaries many of the tools that they are using today against our information systems, and this is an important point that you have to understand while we talk to you about the threat.

Finally, Mr. Chairman, let me say that the concerns that we raise today, although not yet on the front burner, are urgent. In fact, the approach of the year 2000 makes our work all the more critical. It is generally understood that the year 2000 problem poses inherent risks to our system, but it is less understood that the year 2000 also affords special opportunities for our adversaries.

For example, our dependence on foreign software development is a source of concern. It is possible foreign actors with hostile intent may try to exploit the year 2000 problem for their own ends. As we come upon that date, we have to do more than just ensure that our systems function on January 1, 2000, that they function and that they are, indeed, secure.

These are all enormous challenges, Mr. Chairman, and I think we have raised a number of issues that we will want to talk about and I thank you for the time and attention you have devoted to this issue.

[The prepared statement of Mr. Tenet follows:]

PREPARED STATEMENT OF MR. TENET

Mr. Chairman, distinguished Members of this Committee, it is a pleasure for me to come here today to discuss with you a very serious threat to our national security—the vulnerability of our critical information infrastructure to a potentially devastating high tech attack.

Just like the proliferation of Weapons of Mass Destruction, international terrorism, and drug trafficking, information warfare has the potential to deal a crippling blow to our national security if we do not take strong measures to counter it.

Consider for example the *Washington Post* report early this year that eleven U.S. military systems were subjected to an "electronic assault." The perpetrators were not initially known because they hid their tracks by routing their attack through the United Arab Emirates computer systems. While no classified systems were penetrated and no classified records were accessed, logistics, administration and accounting systems were accessed. These are the central core of data necessary to manage our military forces and deploy them to the field. In the end, we found two young hackers from California had perpetrated the attacks via the United Arab Emirates under the direction of a teenage hacker from Israel.

This should not surprise us. A recent DoD study said that DoD systems were attacked a quarter of a million times in 1995. As a test, a Defense Department organization that same year conducted 38,000 attacks of their own. They were successful 65 percent of the time. And 63 percent of the attacks went completely undetected.

We have spent years making systems interoperable, easy to access, and easy to use. Yet we still rely on the same methods of security that we did when data systems consisted of large mainframe computers, housed in closed rooms with limited physical access. By doing so, we are building an information infrastructure—the most complex the world has ever known—on an insecure foundation. We have ignored the need to build trust into our systems. However, simply hoping that someday we can add the needed security before it's too late is not a strategy.

In this hearing today, Mr. Chairman, I hope to leave you with three key points. First, I want you to take away an appreciation for the growing seriousness and significance of the emerging threat to our information systems. Second, I want to emphasize the need to evaluate the threat from the perspective of both State and non-State actors—proliferation of malicious capabilities exists at every level. And finally, I want to provide you with an appreciation for what the Intelligence Community is doing to combat the problem. On this last point, let me assure you that our engagement in infrastructure protection extends not just to efforts within the intelligence community but to participation with all the other stakeholders in our Nation's infrastructure systems—across government agencies, in academia and in the private sector.

Growing Dependence on Information Systems

As this Committee well understands, we have staked our way of life on the use of information. We rely more and more on computer networks for the flow of essential information. Like electricity, we now take information infrastructures for granted. Reliability breeds dependence—and dependence produces vulnerabilities. Today, as a result of the dramatic growth of and dependency on new information technologies, our infrastructures have become increasingly automated and inter-linked. Disruptions in information—based technologies can range from being a serious nuisance—as we saw just weeks ago when the loss of a single satellite caused a nationwide halt in electronic pager systems—to potentially disastrous. Consider what such a disruption would have caused in Operation Desert Storm, where our information systems had to accommodate a communications volume of 100,000 electronic mes-

sages and 700,000 telephone calls a day. Seven years later, those figures would be far greater and our reliance on computers is much greater as well.

It is in this context that we must appreciate that future enemies, whether nations, groups, or individuals, may seek to harm us in non-traditional ways. Non-traditional attacks against our information infrastructures could significantly harm both our military power and our economy.

Who would consider attacking our Nation's computer systems? Yesterday, you received a classified briefing answering this question in some detail. I can tell you in this forum that potential attackers range from national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers, and disgruntled or disloyal insiders. Each of these adversaries is motivated by different objectives and constrained by different levels of resources, technical expertise, access to target, and risk tolerance.

And why would we be attacked? There are plenty of incentives:

- Trillions of dollars in financial transactions and commerce moving over a medium with minimal protection and sporadic law enforcement;
- Increasing quantities of intellectual property residing on networked systems;
- And the opportunity to disrupt military effectiveness and public safety, with the elements of surprise and anonymity.

The stakes are enormous. Protecting our critical information infrastructure is an issue that I am deeply concerned about and requires attention from us all.

Threats from Foreign States

As I recently testified before the SSCI in January, we have identified several countries that have government-sponsored information warfare programs. Foreign nations have begun to include information warfare in their military doctrine as well as their war college curricula with respect to both offensive and defensive applications. It is clear that nations developing these programs recognize the value of attacking a country's computer systems—both on the battlefield and in the civilian arena.

The magnitude of the threat from various forms of intrusion, tampering, and delivery of malicious code is extraordinary. We know with specificity of several nations that are working on developing an information warfare capability. In light of the sophistication of many other countries in programming and Internet usage, the threat has to be viewed as a factor requiring considerable attention by every agency of government. Many of the countries whose information warfare efforts we follow realize that in a conventional military confrontation against the United States, they cannot prevail. These countries recognize that cyber attacks—possibly launched from outside the United States—against civilian computer systems in the United States—represent the kind of *asymmetric* option they will need to "level the playing field" during an armed crisis against the United States.

Just as foreign governments and their military services have long emphasized the need to disrupt the flow of information in combat situations, they now stress the power of "Information Warfare (IW)" when targeted against civilian information infrastructures. The three following statements, all from high-level foreign defense or military officials, illustrate the power and the import of information warfare in the decades ahead.

- For example, in an interview late last year, a senior Russian official commented that an attack against a national target such as transportation or electrical power distribution would—and I quote—". . . by virtue of its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction."
- An article in China's "People's Liberation Daily" stated that—and I quote—"an adversary wishing to destroy the United States only has to mess up the computer systems of its banks by hi-tech means. This would disrupt and destroy the United States economy. If we overlook this point and simply rely on the building of a costly standing army . . . it is just as good as building a contemporary Maginot Line."
- A defense publication from yet a third country stated that "Information Warfare will be the most vital component of future wars and disputes." The author predicted "bloodless" conflict since, and I quote, "information warfare alone may decide the outcome."

As these anecdotes clearly demonstrate, the battle-space of the information age will surely extend to our domestic infrastructure. Our electric power grids and our

telecommunications networks will be targets of the first order. An adversary capable of implanting the right virus or accessing the right terminal can cause massive damage.

Information warfare is not just about offensive capability, however, but about defensive readiness as well. This fact has not been lost on others. Many nations—several of which are potential adversaries—are reviewing their own growing dependence on information systems, both for military and civil activities. They are searching out their vulnerabilites and developing approaches to protect themselves. We must do the same. If not, we could soon find ourselves at a significant disadvantage in addressing what may be the key security challenge of the next decade.

Next—I want to examine the degree to which this threat has proliferated beyond traditional nation states to become the potential weapon of choice for less structured adversaries.

Terrorist Use of Information Warfare Tactics

Terrorists and other non-state actors are beginning to recognize that Information Warfare offers them new, low cost, easily hidden tools to support their causes. They too will see the United States as a potentially lucrative target. These people will be very difficult for the United States to trace in cyberspace.

Terrorists, while unlikely to mount an attack on the same scale as a nation, can still do considerable harm. What's worse, the technology of hacking has advanced to the point that many tools which required in-depth knowledge a few years ago have become automated and more "user-friendly." It may even be possible for terrorists to use amateur hackers as their unwitting accomplices in a cyber attack.

Cyber attacks offer terrorists the possibility of greater security and operational flexibility. Theoretically, they can launch a computer assault from almost anywhere in the world, without directly exposing the attacker to physical harm. Terrorists are not bound by traditional norms of political behavior between states. While a foreign state may hesitate to launch a cyber attack against the United States due to fear of retaliation or negative political effects, terrorists often seek the attention—and the increase in fear—that would be generated by such a cyber attack.

Established terrorist groups are likely to view attacks against information systems as a means of striking at government, commercial, and industrial targets with little risk of being caught. Global proliferation of computer technology and the open availability of computer tools that can be used to attack other computers make it possible for terrorist groups to develop this capability without great difficulty.

Terrorists and extremists already are using the Internet and even their own web pages to communicate, raise funds, recruit and gather intelligence. They also will use it to launch attacks against their adversaries. They may even launch attacks remotely from countries where their actions are not illegal or with whom we have no extradition agreements.

- Let me give you a few examples of what I am talking about. A group calling themselves the Internet Black Tigers took responsibility for attacks last August on the E-mail systems of Sri Lankan diplomatic posts around the world, including those in the United States. Italian sympathizers of the Mexican Zapatista rebels crashed web pages belonging to Mexican financial institutions. While such attacks did not result in damage to the targets, they were portrayed as successful by the terrorists and used to generate propaganda and rally supporters.

Detecting Information Operations Attacks Launched Against the United States

Mr. Chairman, as terrorists and other adversaries well know, our society is based on the free flow of information. That concept is clearly embodied in the Constitution. It forms the foundation of our freedoms and of our productivity. Consequently, our systems are built to facilitate access and openness and they must remain so within the reasonable bounds of security. It is just that openness, however, that makes our systems so vulnerable.

So how will we detect an attack in this world of vast inter-connectivity? It will not be easy. In the first place, those who would attack us, generally, are tough intelligence targets. Second, they will use cheap, easily available technology and techniques. Patterns will be difficult to spot. Furthermore, intrusion detection technology is still in its infancy and the systems we will need to observe are very diverse. When attacks are detected, the source of the attack will be disguised. Moreover, after trouble is detected, it takes time for an analyst to determine whether the problem took hold by accident or by design. Unless we have intelligence indications dealing with someone's *intention* to attack, such as through a human source, tactical warning will be very difficult to attain.

However, by combining the efforts of government and industry, we will be able to pool our strengths and share the necessary information to allow a reasonable defense. Furthermore, by sharing the research and development burden between the public and private sectors, we each will be better able to take advantage of the other's expertise. That is one of the advantages of connectivity.

The Intelligence Community Response

Protecting our systems will require an unprecedented level of cooperation across government agencies and with the private sector. That cooperation already has begun. I view the report of the President's Commission on Critical Infrastructure Protection as a defining moment in identifying vulnerabilities in our 9information infrastructure, in assessing the potential threat to our national security, and in establishing the requirement as well as the momentum for a coordinated effort on information operations. The intelligence community engaged actively in the preparation of that report as well as in publishing the National Intelligence Estimate on Foreign Threats that served as the companion piece to the Commission's report. In producing the NIE, the intelligence community enjoyed extensive interaction with representatives from law enforcement and DoD information security agencies to assess the threat to our computer networks.

These two documents—the NIE and the Commission report—have provided the impetus for significant activity in both the public and private sector to combat the threat to our computer systems. The attention directed to the threat to our information security systems also resulted in the stand-up of dedicated activities within CIA, DIA, and NSA. CIA also appointed an Information Warfare Issue Manager, whose responsibility is to focus collection and all-source analysis on the IW threat and to provide an IW center of excellence within the Agency.

As a community, we have also been active participants, together with other information operations stakeholders, in the NSC-Chaired Interagency Working Group that produced the Presidential Directive titled "Critical Infrastructure Protection" and we are now active in the NSC Critical Infrastructure Coordinating Group tasked to implement that directive. Each of these efforts has had a cumulative effect in building the critical mass that will be required to deal with the threat to our information infrastructure. The Commission report, the NIE, and the recent Presidential Directive will provide the public and private sector with a clear blueprint as to the direction we are taking.

Our very considerable efforts with the Department of Defense have produced organizational, policy and capability improvements and efficiencies for use in information operations. We recently established a senior-level forum to address Information Operations policy and process issues, responding to long-standing congressional interest in the development of just such a policy body. We also created, one year ago, the Information Operations Technology Center at Fort Meade, Maryland. The IOTC is another of our joint DoD and Intelligence Community activities, providing advice and developing techniques that can protect United States infrastructure and systems.

- We have also actively participated in DoD War Games like the Evident Surprise series established by U.S. Atlantic Command and incorporated the threats posed by information warfare into an increased number of other exercises. After my testimony, you will hear from General Minihan, Director, National Security Agency, about the U.S. Government's cyberwar exercise, "Eligible Receiver." Eligible Receiver was an information war wake-up call of the highest order. It highlighted in very clear terms the importance of today's hearing and the work that still lies ahead.

Finally, we must recognize that law enforcement and the private sector are essential parts of our response to this emerging threat. Our Intelligence Community's information warfare efforts include support to the Department of Justice's National Infrastructure Protection Center which was commissioned in response to recommendations of the President's Commission and the joint efforts of the NSC Interagency Working Group on Critical Infrastructure. We are very much engaged in providing technical, analytic and management personnel to the Center as well as needed intelligence support. The NIPC will provide the very critical bridge between government and the private sector. As you know, the private sector is being "hit" every day by hackers. We need to do more to inspire the confidence to work together and to share information with industry to learn more about these attacks, to discover whether they emanate from foreign sources and to become partners in developing the technology required to deflect future attacks.

The Challenge to Act

Mr. Chairman, the concerns we raise today—although not yet on the front burner in the minds of many Americans—are, in fact urgent. We have to focus on this threat now.

In fact, the approach of the year 2000 makes our work all the more critical. It is generally understood that the "Year 2000 Problem" poses inherent risks to our systems, but it is less understood that the Year 2000 also affords special opportunities for our adversaries. For example, our dependence on foreign software development is a cause for concern. It is possible foreign actors with hostile intent may try to exploit the Year 2000 Problem for their own ends. As we come upon that date, we have to do more than just ensure that our systems function on January 1, 2000, but that they function and that they are secure.

These are enormous challenges. As we all recognize, Information Warfare defies conventional and even many unconventional intelligence methods. Intelligence disciplines traditionally have focused on physical indicators of activity and on mechanized, industrially-based systems. With the advert of Information Operations, we are faced with the need to function in the medium of "cyberspace" where we will conduct our business in new and challenging ways.

At the end of the day, the Intelligence Community must be positioned to provide warning of cyber-threats. This warning must go to national leaders and the military of course. But we also must develop ways and means to warn the private sector and the leaders of our economy.

However, our efforts must extend beyond warning. As a nation, we will need to detect attack, withstand assault if launched successfully against us, and then aggressively prosecute action against the attackers. The Intelligence Community cannot do all this alone, nor can the Department of Defense, nor can the Department of Justice or private industry. In this new world of cyber-threats, we will need to work together in partnerships unlike any in our history.

Mr. Chairman, we have made a solid beginning, but we have a long way to go. I appreciate your efforts to bring this vital issue before the public and for your interest in our work in the Intelligence Community. Protecting our infrastructure is a topic which will only grow in importance as we enter the 21st century. It concerns all of us. I look forward to working with you in the future as we build on the foundations we are laying today.

Chairman THOMPSON. Thank you very much.

Lieutenant General Minihan.

TESTIMONY OF LIEUTENANT GENERAL KENNETH A. MINIHAN, DIRECTOR, NATIONAL SECURITY AGENCY

General MINIHAN. Sir, thanks for inviting me here this morning. I was asked to talk about Eligible Receiver and I would like to nest my discussion about Eligible Receiver and characterize it perhaps as a wake-up call in the context of some of the valuable lessons learned which we took out of Eligible Receiver.

As the Mr. Tenet has mentioned to you, generally speaking, the network is an open party line, and I will mention to you several times that what we are really concerned about is the content in the network, not just the network and its security, and that is why the security services that the Director discussed are important.

Having said that, you would expect Defense to test the security services in that network, and that is what Eligible Receiver is all about. We understand that our vulnerabilities have begun to shift from the industrial base or the force structure, which we normally talk about, to our information infrastructure, and the vulnerabilities that are there are shared among government, commercial industry, and in many cases, our allies.

So in the information age, our society is becoming increasingly knowledge-centric and it is that content that is becoming vulnerable to exploitation. It is the content in the network which actually

makes it interesting to conduct the kinds of operations both of you mentioned in your opening comments.

Our network connectivity is continuing to expand exponentially, so as our reliance in these systems grows as a Nation, we are actually increasingly dependent on the information technologies to keep our economy competitive, our government both effective and efficient, the defense system at work, and our citizens safe and secure.

Now, while these advantages of electronic commerce are growing, our technical ability to network has outpaced our ability to protect those networks. Thus, we present our adversaries with an opportunity to gain access to our national security interests. The United States no longer has the traditional sanctuary of a geographically-based industrial base to protect. It also must protect its geopolitical and its global information infrastructure.

So there are no borders in cyberspace and attacks against our networks can come from virtually any point in the globe. Like in real estate, it is location, in this business, it is access, and where the access occurs is where your vulnerability is, so a very complex set of matrices are occurring.

Now, the resources at risk include not only the information stored on the network, but that information which is traversing the network, but also all of the components of our national infrastructure that depend on that information technology and the timely availability of that from an accuracy perspective.

So as noted last fall by the President's Commission on Critical Infrastructure Protection, these include telecommunications infrastructure itself, our banking and financial institutions, the North American power grid, other energy systems, such as oil and gas pipelines and transportation networks, water distribution, and oftentimes we talk of it in segments, like banking, like transportation, but quite frankly, they are all technically all networked together and so they all have shared vulnerabilities, police, fire, rescue, and government operations at all levels.

So as the complexity increases, the issue of interconnectivity and the resultant critical vulnerabilities, as well as deficiencies in our own ability to respond effectively during these kind of exploitations, were really demonstrated in the no-notice exercise called Eligible Receiver 97, which was conducted in June of last year.

Eligible Receiver 97 was the first large-scale exercise designed to test DoD's ability to work with other branches of the government to respond to an attack on the national information infrastructure. In Eligible Receiver 97, information technology knowledgeable people, using open source information and operating consistent with the statutes and regulations of the Nation, successfully penetrated DoD's networks, impacting upon DoD's ability to respond with the use of military force.

Eligible Receiver showed what could be done against segments of the defense information infrastructure and the national information infrastructure with publicly available tools. Eligible Receiver 97 did not constitute a full-scale, state-of-the-art information operations or information warfare campaign. A sophisticated adversary could develop and use more advanced tools and dedicate greater resources and time to support his campaign. In short, our adversaries

will have opportunities and advantages that were not available to Eligible Receiver as the red team.

The last thought I would like to share with you is that our vulnerabilities provide our adversaries with what you refer to as a window of opportunity for an electronic Pearl Harbor, and I think that is a correct characterization and Eligible Receiver is the wake-up call for that concern. I think it is important to see the threat in two contexts.

First, the unstructured threat is the random and relatively limited hacking which you have heard about. It consists of adversaries with limited funds and organization and short-term goals. In some cases, they want publicity. While it poses an important threat to system operations, national security is not necessarily targeted or threatened. This is the most obvious threat which we see today. This threat comes from both foreign and domestic groups, as the DCI has mentioned, and individuals with a range of motives and targets around the Nation—military, banks, public switch network, universities, and corporations. These tactical-level attacks occur every day and will continue.

But this unstructured threat is really providing the tip of the iceberg for what we should really be concerned about, and that is the kind of activity that we would describe as a structured threat. It goes beyond the hacker, but the hacking activity is hiding the more sophisticated set of operations.

At the other end of the spectrum is the structured threat. It is considerably more methodical. It is well supported. These adversaries have all sorts of intelligence support, extensive funding, organized professional support, and long-term goals. For national security purposes, we are concerned primarily with the structured threat, since that threatens our system's survival, while we pay close attention to the other instances which you have referred to in your opening statements.

The information age may require us to expand our traditional concept of what we think of as weapons of mass destruction. Information attacks, when conducted at the strategic level, have the potential to be devastating and the price of admission is considerably less.

If you think about the development of nuclear weapons, they require knowledge plus extensive resourcing and funding and very difficult and hard-to-get materials. Biological weapons also require specialized knowledge, but are less expensive and the materials are more easily obtainable. Information attacks require knowledge and even less funding.

So those fewer dollars actually allow our adversaries to have a greater substantial impact, asymmetric to their own force structure, as they look to disrupt or influence U.S. civil or military activities through the manipulation of our information networks without necessarily directly confronting conventional U.S. military power. This will become an increasingly attractive option for them as we enter the 21st century, and we perhaps ought to consider adding information infrastructure threats to our definition of weapons of mass destruction.

Now, lastly, I would just like to share that we are well into the era of conflict in the information age. This is not view graph engi-

neering. Unstructured attacks are occurring against our networks every day, but unfortunately, most of them are not detected and reported. Consequently, we have no indication of how many attacks are actually occurring and where those attacks are taking place. We face increasing numbers of more sophisticated adversaries if we do not focus on the water beneath the tip of the iceberg.

Peace, as we have traditionally known it in the industrial era, will not exist in the information age of the 21st century. Like our body's immune system, which is constantly under attack, so, too, will our information technology infrastructure be under constant attack. We will need the equivalent of a robust immune system to provide security services that the Director has mentioned to protect our vital organs so that we can enjoy the benefits of the information age in the 21st century.

Sir, I look forward to answering some of your questions this morning.

[The prepared statement of Lt. General Minihan follows:]

PREPARED STATEMENT OF LIEUTENANT GENERAL MINIHAN

Introduction

Mr. Chairman and distinguished Members of the Committee, I am pleased to provide testimony on the broad array of threats users of networked information systems face today from exploitation of their vulnerabilities by a wide array of malicious actors—including hackers, terrorists, and nation states.

The world of the 21st century will look significantly different from that of today. Post-Cold War Russia continues to pose a threat to U.S. national security interests, albeit in new and different ways. China, too, remains a power to be reckoned with. But at the threshold of the 21st century, the true threats to U.S. interests no longer reside exclusively in individual geopolitical entities. As a direct result of the diffusion of power following the end of the Cold War, threats to U.S. security today look very different from those of only a few years ago.

With the dissolution of the Cold War bi-polar power structure, the world's attention has focused on ethnic disputes, the reigniting of tribal wars, and transnational actors. Our policymakers, diplomats, and military forces face more regional conflicts, more peacekeeping operations, and more operations-other-than-war than ever before. Unprecedented transnational security challenges confront the Nation in the form of terrorism, drugs, and international organized crime. U.S. policymakers and law enforcement officials must decide how to confront terrorists, narco-traffickers, and international organized crime cartels that threaten to disrupt the fragile, emerging new world order. These opportunists, enabled by the explosion of technology and the availability of inexpensive, secure means of communication, pose a significant threat to the interests of the United States and its allies.

As was graphically demonstrated by the Department of Defense's (DoD)'s experience in Exercise Eligible Receiver 97, and more recently with the high-profile computer intrusions dubbed Solar Sunrise, we face increasing risks to U.S. interests in cyberspace. United States dependence on, and worldwide connectivity through, this relatively new medium increase our exposure to traditional adversaries and a growing body of new ones, many of whom are fast developing their capabilities to exploit and disrupt networked information systems. The ability of adversary groups and nation states to disrupt or influence U.S. civil and military activities through manipulation of our information networks, without having to confront directly traditional U.S. military power, will become an increasingly attractive option for them as we enter the 21st century.

As a Nation, we are increasingly dependent on information technologies to keep our economy competitive, our government both effective and efficient, our defenses at the ready, and our citizens safe and secure. Unfortunately, these same information technologies bring with them a host of exploitable vulnerabilities. Today's internetworked, interdependent information systems allow us to do things not dreamt of 20 years ago, but they also give rise to new threats to our national security, public safety, and personal privacy. The United States no longer has its traditional, geographically-based strategic sanctuary.

Our connectivity to and through cyberspace increases our exposure to traditional adversaries and a growing body of new ones. Anyone with a computer, modem, and

telephone line can make use of a burgeoning array of network sniffers, malicious software, and sophisticated information attack tools to disrupt network operations. Information attacks can supplement or replace traditional military attacks, greatly complicating and expanding the vulnerabilities we must anticipate and counter. The resources at risk include not only information stored on or traversing cyberspace, but all of the components of our national infrastructure that depend on information technology and the timely availability of accurate data. As noted last fall by the President's Commission on Critical Infrastructure Protection, these include the telecommunications infrastructure itself; our banking and financial systems; the North American power grid; other energy systems, such as oil and gas pipelines; our transportation networks; water distribution systems; medical and health care systems; emergency services, such as police, fire, and rescue; and government operations at all levels.

Indeed, the capability of the DoD to carry out its integrated mission of warfighting and peacekeeping is highly dependent upon the interconnected set of information systems and networks we call the Defense Information Infrastructure (DII), which in turn is dependent upon the U.S. network backbone known as the National Information Infrastructure (NII). In today's environment of sophisticated weaponry and rapid, global force projection, the ability to provide accurate information when needed is vital to all aspects of DoD operations. Cyberspace thus serves as an essential national security enabler, but presents us with a critical vulnerability as well.

This issue of interconnectivity and the resultant critical vulnerabilities as well as deficiencies in our ability to respond effectively during such an attack was demonstrated in a no-notice exercise Eligible Receiver 97 (ER97) which was conducted in June of last year. The Eligible Receiver series of exercises are directed by the Chairman of the Joint Chiefs of Staff and are designed to test DoD planning and crisis action capabilities. ER97 was the first large scale exercise designed to test DoD's ability to work with other branches of the government to respond to an attack on the national information infrastructure.

This exercise clearly demonstrated that IO is a real threat to our Nation and that it can be a dangerous one. New methods for exploiting vulnerabilities are being developed by the hacker community with increasing frequency. These tools are widely disseminated and are publicized in open public forums.

The DII information assurance challenges faced by the DoD are shared by the civil and commercial sectors of the U.S. economy. In a very large measure, the DoD is dependent upon our national infrastructure and the services it provides. Information must be authentic, accurate, private, and available when needed. Our information infrastructure must be resistant to cyber attack across the full range of threats from hackers to nation states, and must limit damage and recover rapidly when attack occurs. This requires a "defense in depth" strategy, one which makes it very difficult to penetrate the NII, but also deals effectively with penetrations that occur. Moreover, the highly interconnected nature of the NII requires that assurance measures be applied coherently—the assurance of the entire NII is dependent upon the assurance of all of its individual elements.

Information System Threats Today

Threat refers to the intentions and capabilities of adversaries to exploit or attack information systems. Capability includes not only access to the appropriate technologies and information, but also trained personnel and adequate funding. It is intention that transforms potential threat into active threat. As Exercise Eligible Receiver 97 graphically demonstrated, a moderately sophisticated adversary can cause considerable damage with fewer than thirty people and a nominal amount of money if the systems they are attacking are not adequately protected and defended.

A strategic-level threat is technologically feasible today. The advent of computer bulletin boards and newsgroups has led to the wide and rapid dissemination of attack/hacker tools and techniques. The development of automated hacker tools makes it easier for less-skilled individuals or groups to inflict more damage. In addition, we have little capability today to provide effective Indications and Warning (I&W) of a pending information attack. During the Cold War, the United States developed robust systems to preclude surprise from nuclear and conventional threats. Unlike those areas, a campaign of information attack has few unique observables.

We distinguish two fundamental types of threat. The unstructured threat is random and relatively limited. It consists of adversaries with limited funds and organization and short-term goals. While it poses a threat to system operations, national security is not targeted. This is the most obvious threat today. The structured threat is considerably more methodical and well-supported. While the unstructured threat

is the most obvious threat today, for national security purposes we are concerned primarily with the structured threat, since that poses the most significant risk.

Hackers have been attacking systems quite successfully for a long time. This threat comes from both foreign and domestic groups and individuals with a range of motives. Targets include government, military, banks, the Public Switched Network, universities, corporations, and research institutions. These tactical-level attacks occur every day. DoD's experience in February of this year with the attacks on its unclassified systems, dubbed Solar Sunrise, was a classic example of this form of attack. The attackers used tools and techniques readily available on Internet hacker bulletin boards. Although these attacks were moderately disruptive, the good news is that the vulnerabilities exploited are relatively easily fixed. For this level of attack, both technology and procedural solutions are available today.

The structured threat is considerably more methodical and well-supported. These adversaries have all-source intelligence support, extensive funding, organized professional support, and long-term goals. For national security purposes we are concerned primarily with the structured threat, since that threatens system survival.

The Gulf War served to alert many countries to the value of targeting information systems. They keenly follow U.S. discussions and activities in the realm of Information Operations/Information Assurance. The Chinese present a good example of the structured threat. In 1995 the Chinese military openly acknowledged that attacks against financial systems could be a useful asymmetrical weapon. By 1997 the Chinese military had incorporated computer warfare into an exercise scenario.

We are well into conflict in the information age. We have failed to adequately comprehend this, for a variety of reasons. We do not have a clear or complete understanding of the threat to our information systems. Unstructured attacks are occurring against our networks every day, but unfortunately, most are not even detected. Of those that are detected, even fewer are reported. We are only seeing the tip of the iceberg. Even when attacks are detected and reported, we rarely know who the attacker was. Traceback mechanisms are not fully developed or deployed. This refers to both legal procedures and electronic technology. Consequently we have no indication how many of the attacks we experience may actually be structured attacks. Nonetheless, it is clear from the information we have, that we face increasing numbers of more sophisticated adversaries. At the same time, the development of automated attacks tools has made it easier for less-skilled intruders to do more damage.

Information Assurance—A National Strategy for Information Protection

"Defense in depth" requires that we not only "harden" the protection of information systems, but also conduct an "active defense" of those systems. Such a defense requires that we have the best possible intelligence on the capabilities and intentions of potential attackers, the ability to use that knowledge to deter attacks whenever possible, and the tools and techniques necessary to detect and respond to attacks that do occur—whether by random hackers or by a hostile nation state. In concert with our partners in DoD, the Department of Justice and the Intelligence Community, NSA is aggressively developing a concept of operation for intrusion detection and response, and the tools and techniques required for time sensitive analysis and reporting. As was vividly demonstrated during Solar Sunrise, analysis and response to such intrusions requires the effective use of experts in a variety of esoteric disciplines; a cadre of experts that will have to be expanded dramatically as the challenges to our information systems' security increase over time.

We must all begin to face the challenges inherent in protecting and preserving the NII. The President's recent Directive on Critical Infrastructure Protection (PDD 63) points the way. Many of the solutions being developed for the DII will be useful in protecting and defending other Federal systems, and will have direct application to the NII. PDD 63 calls for the government to lead the Nation by example in the practice of infrastructure protection, and by extension, information assurance. The Deputy Secretary of Defense has publicly stated that the DoD will lead by example within the Federal sector. NSA is widely recognized as one of our country's preeminent expert resources for dealing with the information assurance problem. NSA will continue to contribute all it can to make information assurance for the DII and the NII a reality.

Chairman THOMPSON. Thank you very much, General Minihan.

There is an old custom in politics. When a guy is about the fifth or sixth speaker at an event, he gets up and says everything has been said but not everybody has said it and so he wants to say it, too. Well, a lot of these things have been said, but now the top guys are saying it, and I think that is the importance of today. When

the head of the CIA and the NSA come in and use terms such as urgent and use the Pearl Harbor analogy and so forth, I think that speaks for itself.

I want to commend both of you for taking it upon yourself to come in and try to heighten our awareness and the awareness of the American people about this problem. I know it is the nature of both of your organizations not to be very public about very many things, but you embraced this opportunity, and I must say, you were very, very frank in laying out the nature of this problem. I think it shows a certain amount of confidence that you are on top of it and you are doing something about it.

I know that the President issued a directive on this last month, and it looks as if a lot of serious attention is being given to it. I think that that is commendable. We maybe should have gotten onto it a little earlier, but I think we are onto it now.

Just in summary, the nature of the problem affects both the private sector and our military. Our military is vulnerable from the standpoint not only of people being able to get into systems to gather important information, but from a standpoint of potentially shutting down our defense information systems at an important time. The threats come from all different kinds of groups—from major powers to perhaps lesser countries to rogue groups to organized crime.

Eligible Receiver showed that a handful of people can wreak major havoc. You demonstrated a vulnerability and you have been willing to go public and point out to the American people what our vulnerability is.

I think we are continuing to learn that every coin does have two sides. When you are talking about the interconnectivity of the world economy—where we like to compete for those exports—our technology serve us well, but when Asia sneezes now, we sometimes catch a cold or maybe worse. The same thing is true as far as the information world that we are living in.

We are interconnected not only commercially and not only militarily, but the private sector and the military are interconnected. It is too expensive to build a contained military system where nobody can break into it, so we have to depend on commercial systems, and we have to be connected.

You point out that our challenge can come from abroad and it can go through several different sources and be difficult to trace back. This situation where you thought we were under attack during a recent Iraqi crisis turned out to be two college kids in California and one in Israel. They ran us through several different terminal points here. One was from College Station to Harvard, which is, as I said, probably the first time College Station and Harvard ever had any communications—— [Laughter.]

And to the United Arab Emirates and all the way back again. As I understand, you had to go in and get search warrants at several different places in order to track down these individuals, which is another problem.

So with very little sophistication, an awful lot can be done to damage us, and underlying all of that is the year 2000 problem, which just exacerbates everything else. It is a tremendous problem in and of itself, but when you combine it with computer security,

it is going to make us even more vulnerable, especially in the short run.

I just want to start out by thanking you and the administration for being willing to have you lay out for the American people the very, very serious nature of this relationship and the challenges that lie ahead.

I think Mr. Tenet's most direct comments had to do with the need to work with industry and what he describes as not really an encryption problem. There will be a lot of debate as to the nature of encryption, but you have an industry that is used to disseminating information. You point out that you need to protect information. You have a situation where companies do not want the government coming in and saying, we think we have a problem, open up your records. So you have a search warrant problem in a place where it takes an instant to transfer information around the world. The challenges lie before us and are going to be tremendous.

Let me ask you to focus in on the year 2000 problem for just a moment. There are various aspects of this, as we said. The nature of the year 2000 problem in and of itself is one of them. Are there dangers with regard to critical systems that have military significance, such as nuclear power plants, weapons systems, and so forth, where we are hearing about troubles in some countries, that still have nuclear capabilities? Is there a national security military relevance to this year 2000 computer problem?

General MINIHAN. Sir, there is no question that there is a national security relevance. I would like to put it in a couple or three shades.

First, your awareness exceeds by a wide margin most leadership's awareness outside the United States. So with the exception of a few countries, America is aware and aware at leadership levels significantly beyond any other countries we see. As a result, there is just now an emerging sense of the problems.

Second, there is this sense that, well, the Americans will just issue some software and it will be fixed, so they do not have a sense of the complexity, either. That results in the phenomena you are talking about, where you then begin to worry about the software integration of indication and warning systems for nuclear prepared countries, what are their scopes going to look like. You have seen some instances in the past when the scopes do not work correctly for other reasons, it is confusing and you lose the kind of confidence that you have.

Chairman THOMPSON. You are talking about scopes. What are you referring to?

General MINIHAN. When you are looking at the situational awareness of what is occurring in the world that you would worry about being attacked, and if that scope were displaying inconsistencies with your sense of safety, you might think you were being attacked when, in fact, your software was not acting correctly. So it is a very complex problem to think your way through and they are not nearly at the point that we are in doing it. So we both have the problem——

Chairman THOMPSON. But their problem becomes our problem, does it not?

General MINIHAN. It becomes our problem. So you have, I have seen any number of our leadership now as they travel begin to have exchanges with their counterparts. Are you thinking about Y2K? Have you understood? We are seeing some nice exchanges occur and awareness is growing, but there is much work to be done for us to get to the point where they have the same certification process that we are going through to make sure that their software is in place.

Chairman THOMPSON. Mr. Tenet, do you have a comment?

Mr. TENET. Yes. I think, Mr. Chairman, we have to be careful not to construct catastrophic scenarios, but the fact is, a bank that is unable to transact business in a country that is experiencing financial activities in 2000 and creates greater problems, there is a national security dimension out of that instability. The failure of early warning radars to work because we have not fixed the problem creates an instability in and of itself.

So we are looking at all these things and we are focused on it. As General Minihan says, there has been an uneven appreciation of the application of what needs to be done across the world. It has not been even, and because you're networked the way you are, just because you fixed the problem does not mean you are not going to have a problem.

Now, the Y2K problem also has to be understood in the context of it is the transaction that will suffer. If people do prudent things, they will be able to save data. You will be able to save your bank account. You are not going to lose your money. The issue is, can you conduct a business transaction? If the computer networks have not been fixed to accommodate what needs to be done, that is where the danger lies.

And if you extrapolate onto any of the critical industries that you are thinking about in this country, magnify it overseas and then tell me how stable a country is, tell me where they are in their political process, tell me what their financial situation is and I will paint you a national security dilemma, depending on the country you are dealing with.

General Minihan is right. We are engaging our partners at all levels to talk to them specifically about their Y2K problem. Secretary Cohen has talked to his counterpart in Russia about his problem to ensure that they are focused on it, and there are ongoing discussions, and we, in fact, I think, are driving the boat on this issue as hard as we can because we understand the connectivity issues and what the implications are.

Chairman THOMPSON. Is it fair to say that we really cannot tell where we are going to be in that regard by January 1, 2000, even the extent to which we have been able to address the problem, much less whether a Russian, for example, has been able to address the problem? So when things happen or if unusual things happen, shall we say, along about that time, we will not know whether or not it is by design or whether or not it is a part of the Y2K problem?

Mr. TENET. I think it is fair, sir. I do not think General Minihan and I could paint a picture today that provided you a high confidence accuracy about where we are going to be. We are following the problem, and obviously we have targets we are more concerned

about than others. We can talk about that in a classified session. But it is the unevenness of the application that worries me.

General MINIHAN. Sir, I think you need to accept some level of uncertainty. I always tell the boss that I see this as—Y2K is like the El Nino of the digital age. It is going to come through, and we do not necessarily know all of the patterns that are going to emerge. What we want to do is have an excellent sense of what is really important and protect and fix that, and there will be global addendums to that, which is what you are talking about, so it is not just a United States-only fix.

Whether you wanted to talk about it in the context that you mentioned, nuclear early warning, or whether you want to talk about it in banking or whatever, we need to find those very important areas and work those. You can set those in a condition where you would be relatively certain that your transactions are secure and that you have your data stored. Now you have a range of things you want to work on which may not be in the top range but are still critical and we want to focus on those.

So within a range of things, we are going to have some storms and we want to be able to deal with the storms as they occur, so we have to have a nice emergency service. We have to have the ability to respond. We have to understand what sort of skill basis we need in our various institutions to do that, and again, that will be a global construct, not a United States construct.

Chairman THOMPSON. Right.

General MINIHAN. But I think it would be illusory of anybody to tell you we are going to get our arms around this, it will be OK, and we will guide through it.

Chairman THOMPSON. But the other side of that coin is that we do not want to generalize so much in talking about the various inconveniences and problems and so forth, and by the way, there is a nuclear component out there, also.

General MINIHAN. Right.

Chairman THOMPSON. That is a category in and of itself, and I assume is being prioritized——

General MINIHAN. Yes, sir. That fits up there——

Mr. TENET. Right at the top.

Chairman THOMPSON [continuing]. In terms of addressing these things.

Along those same lines, in terms of the year 2000 problem, a lot is being written about how we are addressing that and the need that we are having to bring in a lot of technical people to address this, both in terms of industry and in terms of the military, and that we are getting or will be getting a lot of our help from various foreign countries. Other countries have been mentioned in the press. India, for example, apparently is going to be supplying a lot of those technicians. Of course, it only takes one person, I would assume, among the thousands to create a real problem, if the wrong person were to get into the wrong place.

What kind of potential vulnerabilities are there in terms of our military, and in terms of our industry, with regard to the concentrated effort that we are going to have to have in order to get enough people in to solve this problem? The way it is explained to most of us is that the technical aspect of it is not all that com-

plicated, but it is a severe manpower problem. It is going to take a lot of people doing a lot of work to fix it. How does that make us vulnerable? What can we do to minimize that?

Mr. TENET. Well, it is a tough problem. I mean, we have a shortage of software engineers. We have an abundance of foreigners who are willing to solve this problem for us. Y2K remediation provides all kinds of opportunities for someone with hostile intent to understand how your computer network works, how your business works, what your vulnerabilities are.

So we are watching it very carefully. We are working with the Bureau to understand whether anybody is organizing a threat, so if we see that kind of an organization, we can then talk to our industry about what we find and what we know. But everybody is in the same boat. It goes back to what your contracting procedures are like, who you are dealing with, who they are dealing with, who makes the code, that every major industrialized country makes this stuff, and that is the world we live in and everybody is in the same boat, Senator, and it is not an easy problem.

Now, we have to be careful, to be very careful not to create the image here that every foreigner that works for you is somehow in the employ of a foreign intelligence service, because, quite frankly—or a hostile terrorist organization, because I do not have the evidence today to sit in front of you and say, there is a massive program to disrupt us. It is intuitive on the basis of the shortage that I just described that people have to take care and we have to work with the Bureau to help you understand if it exists on how to better protect yourself.

We are working along those lines, but this is a big problem. I mean, in some ways, it is a big opportunity, and it is something you may not know about for many years because of the stealth and the sleeping quality of some of the applications people can inject into your systems.

So it comes back to, it always comes back to where are you on the defensive side. What have you done to protect? What is the system security that you have put in place, and it has to go hand in hand with dealing with this problem. If you isolate it, we are going to set ourselves up for a very large problem.

Chairman THOMPSON. General, did you have something you wanted to add?

General MINIHAN. Sir, I would only add that this, I think, will become a normal state of concern. It is not something that just occurs because of Y2K. So we, over a long period of time, are going to have to deal with this, and as you develop the sets of security services, authentication, and what have you, we want to have a rich enough set of variables that you cannot go through all the layers we have set up and exploit us. And when we set those layers up, we have to hierarchically understand, as I mentioned to you, what our real strategic sanctuary is that needs that kind of protection. But as a matter of the normal habit of concern, it is something that is going to be with us in the information age.

Chairman THOMPSON. So we have a challenge on the back end in terms of fixing the problem and then we have a challenge on the front end in terms of heading the problem off, I guess you might say. I take it we cannot have an early warning system that some-

one is going to attack our information systems in the way that we have a nuclear early warning system, which causes me to wonder whether or not we are seeing a situation where human intelligence is going to be even more important with regard to this kind of problem than it has been in the past, both from an intelligence standpoint—early warning, and from a counterintelligence standpoint—what are they doing to us here. Is that a fair assessment?

Mr. TENET. Senator, you are absolutely right. The focus on getting into and determining someone's intent is going to largely be a human intelligence, and a technical intelligence, problem that we face.

There is another side of the equation, as well, which is when I talked to you about shared vulnerabilities. We have all read about all of the anecdotal information and examples of companies being attacked, banks being attacked, and the fact is, none of that information is shared. Now, I understand the proprietary interest that a company or a bank has in not wanting to share that information so that the integrity of the institution is not challenged, but someplace, in some vehicle, that information has to be shared so that we can understand the nature of what is going on so we can differentiate between the hacker and the more organized attack against your infrastructure. And there, I come back to this shared vulnerability and trust between business and industry and government that we simply have not solved yet.

Chairman THOMPSON. Senator Lieberman.

Senator LIEBERMAN. Thanks, Mr. Chairman. I just want to begin by echoing what you said at the outset of your questioning, which is that the testimony of Mr. Tenet and Mr. Minihan is very sobering and troubling. This is not a case where you have come in and diminished our concerns. I do not believe you are overstating it. You are not encouraging us to panic. But you are telling us there is a real problem. In a sense, you are confirming our own intuitive fears about this, and in that sense, I thank you for being so direct.

Mr. Tenet, you have described in your testimony the Eligible Receiver demonstration exercise as, "an information war wake-up call of the highest order," because it showed a vulnerability. So we are on notice and we all ought to work together to try to figure out how to reduce the vulnerability, understanding that we live in a world where risk is part of life, and in some cases, the best we can do is to minimize the risk and then try to defend against it.

I want to see if I understand at this point where we think that the most significant threats come from. Would you say that they are at this stage from nation states or are they from terrorist groups or criminal syndicates, for instance?

Mr. TENET. Well, at this point, Senator, what you have is all the anecdotes we know about are not affiliated, to the best of our knowledge, with nation states or intelligence organizations. The hacker phenomenon, basically, what I think it is what it will create is a copycat mentality and people will watch. The organized structure, government, services, groups, are watching to see what our reaction is, watching to see how we attempted to solve the problem, looking at the facility with which these things occurred.

Nation states today, and the programs that we talk about in our estimate, really are focused on military applications and military

doctrine and conflict. How do you bring down somebody's air defense system? How do you bring down traditional military kinds of targets?

Senator LIEBERMAN. Right.

Mr. TENET. All of that is transportable to a more sophisticated kind of warfare down the line. So the reason, I think, we have got some time and hope here is that we have time to get on top of this problem, to anticipate how this will naturally migrate, because for nations, there is enormous technical prowess and capability that is involved in mounting an attack against us. They are now starting to think about it, write about it, incorporate it in their doctrine and develop capability.

Senator LIEBERMAN. Right.

Mr. TENET. That has to be matched with the defensive side on our end so that we can be ahead of the curve. I have not seen evidence to match up the anecdotal evidence that you and I have heard about in these break-ins to a government or a program that is very large at this point. So we have not had that match up occur yet. We have seen terrorist groups express interest in this kind of technology, because they understand the anonymity and the facility with which we can do this, but we do not have evidence to suggest that, aside from the two instances I cite, that it has occurred yet. It does not mean it will not.

Senator LIEBERMAN. Which are the Zapatistas and the Sri Lankan case, right?

Mr. TENET. Right. The point is that your point about let us not get panicked is the right point. The threat is real and what people learn from this is quite real. So down the line, I think we are going to encounter more of it and it will be more organized.

Senator LIEBERMAN. I think part of what you are saying is that at this point, we have no evidence of an attempt to attack us through information warfare or even to test our vulnerability by a nation state or a terrorist group.

Mr. TENET. Let me make that distinction.

Senator LIEBERMAN. Go ahead.

Mr. TENET. In terms of these incidences that we know about, we know that that is not the case. We know, and I think we talked to you about in the classified session—I want to be careful—that there is at least one instance where we think there is an active targeting effort.

Senator LIEBERMAN. An active——

Mr. TENET. An active targeting effort underway of U.S. information systems.

Senator LIEBERMAN. Right.

Mr. TENET. But, you see, we have not migrated to the far end of the spectrum yet, so it is moving.

Senator LIEBERMAN. And from your testimony, it is clear that we do know that there are nations in the world who are developing information war capacity.

Mr. TENET. Yes.

Senator LIEBERMAN. You mentioned Russia and China. Let me be careful about what I am saying. You quoted in your testimony individuals from both Russia and China who were speaking, at least theoretically or at least strategically, about the potential im-

pact of information warfare. Those are large countries. They are countries with which we have—it is much in the news today—with which we have non-hostile relations. Do we have reason to believe that the development of information war capacity in those two countries, for instance, is in some sense targeted at us, or is it just an exploratory——

Mr. TENET. Well, I think what we have described, Senator, is it is natural to see in someone's military doctrine and thinking this kind of thinking, in terms of being aware of what the phenomenon will afford you someplace down the line.

Senator LIEBERMAN. Right. I do not want to——

Mr. TENET. I do not want to cross lines here.

Senator LIEBERMAN. Understood. And again, I do not want to tread over the lines, so you can tell me if you cannot answer this next question, but I wonder about some of the smaller countries with whom we have clearly hostile relationships, such as Iraq, Iran, and Libya.

Mr. TENET. Well, let me answer the question in this way. In all of those places, we see those countries enhancing their computer capability and their connectivity and acquiring more and more tools, so you have to worry about how they take these civilian applications and then think through how they might apply them or transfer them, in the case of rogue states, to terrorist groups for some application against the United States.

Senator LIEBERMAN. Right.

General MINIHAN. Senator Lieberman, may I offer a thought?

Senator LIEBERMAN. Yes, please, General.

General MINIHAN. I mentioned in my testimony, I prefer to enter the discussion as conflict in the information age, and I mentioned to you that it is the content in the network which is what we really worry about in terms of vulnerabilities. Information warfare in the context that we have been discussing is, in my view, a portion of that, but you also have a wide menu of other things which can occur in conflict in information age with regard to the information or the knowledge which you have, which may——

Senator LIEBERMAN. Give me an example of what you are thinking of.

General MINIHAN. I was smiling to myself as you were—I, too, talk to my kids on E-mail and they are a lot closer than I want them to be, but my experience is not like yours. It is not cheaper, it is more expensive because my daughter says, "Send me money, Dad." [Laughter.]

Senator LIEBERMAN. So that is the content.

General MINIHAN. The content is about money. She does not know. I do not know who is asking me for the money. I do not know where the money went when I send it, and I do not know if—she says, just send it to You Pick It because I bought a new outfit. I do not know if all that has occurred until after the fact. Well, I am vulnerable in that economic transaction and there are people who would take advantage of that vulnerability.

So conflict in the information age has a much broader sense, and the Director is absolutely right. There are militaries thinking their way through the military application, but I think at your level, we

are going to see it as a much more substantial issue than just information.

Senator LIEBERMAN. That is a good point, and I appreciate your making the point.

Before I get to what might be done to defend against this threat, I think it is important for the public that will hear about this hearing and our concern about this, and again, I understand that you can only say so much in an open hearing, to understand that we in the United States also have information war capacity. In other words, we have not decided to disarm here. We have a developed information warfare offensive capacity. At the level of generality that you wish to address it, can we assure people of the country that that is true?

Mr. TENET. Well, we are the wrong people to ask, but we can assure them that we are not asleep at the switch in this regard.

Senator LIEBERMAN. That is certainly my understanding. I mean, we may want to come back in a bit, and I will, about what extent we can use to try to protect ourselves defensively, but let me come to the issue now that I do not understand, which is as complicated as this problem is—and it is enormously complicated—I was thinking as I was listening to your testimony about the Congressional focus on missile defense, theater and national missile defense, the difficulty there, but it is in some ways, I hate to use the word easier, but we have satellites that are capable of noticing a launch of a missile.

But there are millions of places of origin that are not subject, as I understand it, to conventional satellite radar, whatever, detection systems. Then we have the problem, once the missile gets up, of how do you stop it, and as others have said, it is how do you hit a bullet with a bullet.

Maybe once an information warfare attack is launched, the site of the origin is enormously complicated to detect. Maybe it is somewhat more manageable to stop it, but that is my question. Are there technologies now in existence or being developed that can protect our transportation infrastructure, fiscal infrastructure, military infrastructure from this kind of attack, which is to say an information warfare attack that intends to disrupt or confuse our systems?

General MINIHAN. Sir, I think you asked exactly the right question, and the analogy to missile defense is a good analogy. The industrial age had us think about indications and warning attack assessment and defense and sequencing through that protection side in a physical context, and what we are talking about here is a virtual context.

I was tempted to mention to the Chairman, I would not yield to the point that we cannot do indications and warning. I would say that it will be a substantially, completely different process by which we do indications and warning and attack assessment. So we will develop in cyberspace, just like we have for missile defense, an indications and warnings scheme which allows us to see other networks configuring, who is using it, and be able to defend in cyberspace as opposed to report what has happened from a forensics perspective. We will get to those technologies.

Senator LIEBERMAN. But we do not have it now.

General MINIHAN. Well, I want to take you one more step.

Senator LIEBERMAN. I am sorry. Yes.

General MINIHAN. We are now in the early stages of developing those kinds of technologies. Now, this is where the Director's point about the close relationship with industry is very important. The major industry service providers have a need for the same information, and so we have a shared vulnerability there because we are both riding on the same network, and we have a shared relationship. Neither one of us want to lose the denial of service or whatever. And it is in that scheme where you will start to see the new technologies emerge as we build those relationships.

Senator LIEBERMAN. Are we devoting sufficient resources to developing those defensive technologies? For instance, is Congress giving you and associated agencies adequate resources to deal with this?

Mr. TENET. I think the answer is yes. I think we are getting what we are asking for and we are at the front end of developing a more robust program and there will be more resources required over the course of time. I mean, we are just beginning the effort.

Senator LIEBERMAN. Right.

Mr. TENET. I think we are—I would say we are sound, but I do not think there is any doubt we are going to need more money in the future to deal with this problem.

General MINIHAN. Sir, it is a growth area. I mean, we are going to invest in it, and I think you have got a nice foundation to invest on. My own organization is the National Security Agency, so we also make—and we are investing in that relationship. There are any number of initiatives now to share vulnerabilities with industry and to start to understand the threats—and to start to have mutual investments in understanding that complex protection. So I think we are going to grow into it.

If I could use the phrase scalability with you, if I were worried about something, I think at the end of the day, when you are finished with your third hearing, there will be a cost associated with scaling our protection capability out to a global context, not so much in the technology but in the scaling of it because it will be global, not geophysical.

Senator LIEBERMAN. Right. How about efforts to mitigate the damage once an attack has occurred? In other words, when we are dealing with weapons of mass destruction, chemical and biological, if we have evidence that someone is attempting to smuggle something into the country or even that something has been set off, we have defensive systems. Are those also being worked on here once we have reason to believe an attack has occurred to mitigate the damage?

General MINIHAN. Yes, sir. We have—I am really not the one, but I think you correctly bring together the notion here that we want to defend in cyberspace, not have the forensics of what happened to us. There are any number of organizations within DoD now which look at those characteristics of the network, and you can disconnect yourself from the network just as easily as you can stay vulnerable. So you have some options available if you understand your vulnerabilities and you execute those options at a layer which

still allows you to do the job that you would want to do. We are developing those complexities.

Senator LIEBERMAN. This is an interesting point, and maybe it is one to get to at another stage, but part of the problem here, part of the vulnerability is that we have so remarkably connected computer systems, to our advantage, but as we have all said, that advantage creates vulnerability, and I suppose it does raise a question that we ought to consider, as to whether in some measure we want to separate some particularly vital systems. What do we lose by that and what do we gain in greater security if we do that?

Coming back to our own offensive capability here in information warfare, and this is early thinking, I am sure. We were in a discussion, and I give credit to Senator Glenn because he raised this question in a discussion we had, but we ended up in the Cold War with the Soviets in a so-called mutual assured destruction, which was, in its way, a bizarre, in some sense, totally irrational system, but it seems to have worked, which is do not strike us because if you strike us, we will strike you back at least as devastatingly.

It does seem to me that one alternative we have for a defense here, if you will, is the continued development of our offensive capacity as a deterrent. I do not particularly invite a response, but if you are interested in responding, I would be happy to hear it.

Mr. TENET. I think we will take you up on a non-response. We appreciate the offer. [Laughter.]

Senator LIEBERMAN. The other thing I would say, and then I will yield back to the Chairman, I appreciate what General Minihan said, that leaders, in some sense, our leaders in this country are way ahead of other leaders around the world in considering this problem, and it may be that we want to raise this up at a diplomatic level to begin to discuss it. I do not know whether this is subject to the kind of international diplomacy, treaty making, a kind of new world of arms control, conflict resolution process.

You have given us a warning and it is a very real one and it is here and it is multi-polar and it is relatively cheap to get into. Before long, I would guess, we are going to want to see whether there is some sense in which we can develop some systems diplomatically and in international law to try to at least reduce the vulnerability here.

I was struck, and a final word, General Minihan about your description of Eligible Receiver because it did, I know, show some vulnerability, but it seemed to me that you indicated that this was at what I might call a medium level. It was not an all out, highly sophisticated attack. Is it fair to say that it was carried out with a—I am not asking for details, but with a moderate level of personnel and at moderate expense, so this was not a big budget, big personnel operation, which suggests in another way the range of the threat that we face here?

General MINIHAN. Yes, sir. I would characterize that. The team was less than 50. I gave them a couple of months, and——

Chairman THOMPSON. But highly competent personnel, since some of them are in the room here today, right? [Laughter.]

General MINIHAN. Are the heads going up and down behind me? [Laughter.]

And they understood their business.

Senator LIEBERMAN. Yes.

General MINIHAN. Then we obeyed the law. So, essentially, in the nature of our test, essentially, if I were an adversary, I would not have been under any of those restrictions. I would have taken my time. I would not have just used openly available tools. I would use all of the tools at my disposal. I would have had a team that would have been together for a much longer period of time, and when it was finished, I would have run a legitimate campaign.

Senator LIEBERMAN. Right.

General MINIHAN. And I would like to come back to my other point with you. It would have been part of a larger phenomena of conflict in the information age. That is the other part that Eligible Receiver gives you, is that while this is occurring, there are other things happening in the policy maker and the leader's mind. It is not clear that there is an information warfare component to the Eligible Receiver exercise until you are well into it. It looks like terrorist operations. It looks like you are having mechanical problems with your infrastructure.

Senator LIEBERMAN. Right.

General MINIHAN. It is not a very clear state of affairs for the decision makers.

Senator LIEBERMAN. That is such an important point. For instance, if somebody fires a missile at us, we have a pretty high probability of knowing that there is an incoming missile; not so here.

I gather that during this Cloverdale situation, where the two young people in California working with the person in Israel, who were hackers, if I recall correctly, this happened at a time when we were contemplating, well known to the public, some sort of military action against Iraq because of their noncompliance with the inspection regime, and there was some concern that the evidence of the hacking by the Cloverdale group might have been an initial foray to test our vulnerability to the Iraqis. It was some period of weeks before we were able to discover exactly where this was coming from, so that something was incoming, but it was not clear where it came from or what its intention was. As it turned out, its intention was non-hostile, but that is part of the complexity.

Anyway, your testimony has been, for me, riveting, very helpful, and you all have a lot of work to do. Thank you.

Chairman THOMPSON. Thank you, Senator Lieberman.

Along the same lines, General Minihan, that you were just discussing. It seems if we cannot consider an attack of this nature in isolation or in terms of mutually assured destruction, is it not true that in all probability, that any major military offensive of the future would be preceded by an attack such as this—an information disruption attack—whether or not the subsequent attack was a land war or an air war or a nuclear attack? Would it not stand to reason, or is this getting into something we do not need to get into?

General MINIHAN. No. I just would share with you, if you mean preceded in a sequencing sense, I would nod my head, but I am trying to say it is an inclusive part of an overall effort because our vulnerabilities are not necessarily exactly where we defend. So you are going to attack your adversaries' vulnerabilities. They are not going to attack our strengths, and if our strength is someplace else,

they are going to make that matching, depending upon what their particular interests are.

In this case, in Eligible Receiver, we used it throughout. So it preceded, it was in the middle of the exercise, and we used it at the end. I like to return to lessons learned because you pick up a lot. What is your relationship with law enforcement? How do you do indications and warnings?

We kidnapped a systems administrator in this scenario. Well, a systems administrator for us is the code clerk of the 21st century. The systems administrator understands how the network that you are using is configured. Well, it is a lesson learned, because if we lost a code clerk, we would all immediately react because that would understand—we need to think of your systems administrator in an equally powerful way, so you are getting a lot of that. But there were any number of instances through the exercise like that. It was not something that could just be phased.

Chairman THOMPSON. Sure. Do you have anything to add to that, Mr. Tenet?

Mr. TENET. No, sir.

Chairman THOMPSON. On the ability to develop the technology of the future as you were talking about, I think that is something we naturally look for in this country. We think that if we do not have it, we will soon have the technological ability to deal with it. It is kind of ironic that many of us think that we cannot develop the technology to defend ourselves against a missile but we can develop the technology to defend ourselves against something much more complex.

We are a country that also thought a few years ago that someone would surely come along with some simple way to cure the year 2000 problem and that did not happen. I think that, clearly, we need to do what we can in that regard, but certainly not be sanguine under the notion that we will be able to effectively do it.

Mr. TENET. Mr. Chairman, I feel very strongly about this and I am going to say it again. There is not any technology available to solve this problem unless this country gets about the business of building a system of trust and security for its information network. It is not going to work. The layered approach and the approach that General Minihan talked about, if you want to give us a chance to do the diagnostics and if you want to give us a chance to understand what has happened, then you have got to make it a lot tougher for people to break into the system.

We have all been logjammed on this encryption debate. Nobody is moving in the direction that we need to because we do not have the trust and confidence in government and industry that is needed and the consequences are that our vulnerability increases every day. People have to get off the dime and understand that some system based on trust, a key management infrastructure that assures authentication and integrity and non-repudiation, starts to be built or we are not going to have the tool at our disposal that we need to minimize and isolate these attacks to understand them. We will not be able to deliver.

Chairman THOMPSON. You have come back to this a time or two and you speak with passion on this point, so I want you to elaborate on this a little bit. I think the American people need to under-

stand this. Tell us what you perceive to be the nature of the situation today between the competing interests, if you want to call them in competition--between industry and the private sector on the one hand and the government on the other.

We are all aware of the fact that there is an encryption debate going on and different people have different ideas. But elaborate if you would on where you see the debate standing today and then take us to where you think we are going to have to go, because you clearly think that that is the key. So elaborate on that for me.

Mr. TENET. Well, Senator, I did not mean to be so passionate, but anyway—— [Laughter.]

Chairman THOMPSON. No, that is good.

Mr. TENET. But in any event, there is an ongoing debate between industry and government about what to do about encryption, and at the heart of it is there is a lack of trust.

Chairman THOMPSON. Now, for those who are watching here, describe the encryption situation a bit, just for the layman.

Mr. TENET. Go ahead.

General MINIHAN. Sir, we have had a discussion, I think legitimately, in the past, which begins with our transition from a technological perspective, from our ability to protect ourselves with hardware, known as Clipper Chip and things like that, black boxes, to what became available, which is commercial software and commercial products, which can also be used to protect ourselves and are not necessarily government produced and government owned, as earlier.

As we go through that transitional period, which is normal, we focused on the encryption that would be a part of that product. I am going to use the word "product". As a result of that focus on that product, encryption, what the Director is suggesting is——

Chairman THOMPSON. What is encryption?

General MINIHAN. Encryption is the technology which allows us to scramble the information so that if I sent my money to my daughter and you intercepted it, you would not be able to tell what I was doing. It was secure.

Chairman THOMPSON. All right.

General MINIHAN. Now, what has occurred by having that masking debate, and I mean that in a positive way, what we miss is what we need is a discussion about a national information assurance strategy, just like you referred to in mutual assurance. What is the Nation's strategy, Federal, State, and local, since all of those components are there, and encryption is one service I would like, security. I also want authentication, digital signature. I want assured connectivity. I would like to know when the transaction is complete. And I want to know that no one messed with this transaction when it was being sent.

That rich set of security services is a product line which is much more substantial than the encryption discussion allows you to look at, and what I think we want to do is broaden the debate so that there is a trusting relationship in building those product lines.

The services that are merged, the services that Senator Lieberman and I need to talk to our family, the kinds of things which naturally go, and when we build that, then we start to build this national information assurance strategy which then lets you,

I think, focus on who is going to do indications and warnings, what is going to be the nature of the investment across it, what are the relationships that you would like between industry and government in the context of sharing information——

Chairman THOMPSON. Which is a separate debate about the sale of encryption devices in and of themselves.

General MINIHAN. There is not. The debate of the sale in that sense is twofold. Americans produce a very strong encryption product and there are two components to its sale. One is we do not want Iran to have a product like that. A rogue nation or somebody should not—technology transfer, like in nuclear—that is why I suggest you may want to add information technologies to weapons of mass destruction. We would not want rogue nations to have strong encryption built by the United States.

The second part is, there is an international component which says that the two nations, the one building and the one receiving, need to agree on the kind of product they would like. So there is an enabling portion to it, also, which needs to be——

Chairman THOMPSON. A lot of people say that in encryption, the genie is out of the bottle and you cannot control it anyway and if we do not sell it, other people will, just to lay a little groundwork.

Mr. Tenet, I know you had some additional comments.

Mr. TENET. The only thing I would say is the other issue that is out there is should this information be recoverable in some way, shape, or form, for example, by the law enforcement. The Director of the FBI has a terrible problem on his hands. Let us assume for a minute—let us replay the World Trade Center. Let us assume for a minute that he gets a court order that allows him to access the communications of a terrorist group. Let us assume for a minute he gets access to the communications but he cannot access the contents of those communications because they are encrypted. The building blows up. Thousands of people are killed and he has no guaranteed access.

The whole question of how you recover information out of the encryption debate is important. One man's privacy is another, the Director of the FBI's, requirement to gather information. How do you protect the privacy and rights of Americans and at the same time protect the ability of the law enforcement community to do its job, and that is where the issue has been joined.

As the Director of the CIA, let me give you another example. Let us assume for a minute I give my employees the ability to encrypt their information. Let us assume, God forbid, something untoward happens, an illegal activity occurs. By virtue of encrypting their information, they have also destroyed that information and I have no ability to recover it.

Or in companies, people engage in conspiracy theories and activities and collude to commit crime against a major corporation and they encrypt that conspiracy within their computer networks in their business and the chairman of that company has no way to recover that data.

Now, I would say to you that that is not a tolerable situation for either the private sector or the law enforcement community, and we are either going to do this voluntarily, we are going to work through this together and try and get it done, or we are going to

get a major terrorist event and we are going to mandate it. Now we are all dancing around each other trying to figure out what the right way to do this is.

Well, there is a right thing to do for the country and we have to work out how to recover that data, whether it is by key escrow or other means, but there is a train wreck ready to happen unless we deal with the recovery piece of this encryption debate. It sure is going to happen.

Chairman THOMPSON. On that particular point, it raises the question concerning our potential assistance of other countries with regard to encryption, which brings us to supercomputers. As you know, there has been an ongoing discussion as to the extent to which we should be supplying certain so-called supercomputers to other countries, such as China. Some people are concerned that we are giving them information, we are giving them technical information, encryption information, that would be useful to them in ways such as you discuss. Do you have any opinion with regard to our policies concerning the sale or transfer of these supercomputers to other countries?

General MINIHAN. Sir, it is certainly not mine to do from a policy perspective, but I would share with you two thoughts. One, remember that it is the content that we are interested in, and so the supercomputer, to the degree that it enhances your ability to work in that environment, would be what we would want to think about, not just the fact of. And so you want to see, I think, those kinds of decisions in a policy sense that are very complex, not unlike the technology transfer policy of the 20th century, where it looked at what does it contribute to, and you want to have a very complex discussion about it.

Second, to get back to your genie-out-of-the-bottle thought, it is the sense that when you have these product lines which occur, that they have to be usable across international boundaries, and if they are not usable in a wide variety of contexts, then we are not going to be able to take advantage of them and the genie is not out of the bottle because we are unable to take advantage of these commercial products in a larger sense because we do not have the security services in which we can wrap that product line. So the real commercial aspects of this awaits a nice robust set of security services.

Chairman THOMPSON. Senator Lieberman, did you have another question?

Senator LIEBERMAN. Just very briefly, Mr. Chairman, about the encryption debate. I think that the discussion that General Minihan and Mr. Tenet have had with you has been very helpful, and in one sense, it at least brings to my mind how complicated this all is, because we have tended to think about the encryption problem as one that can be a frustration to law enforcement for the obvious reasons that you have stated, where law enforcement has had access to telecommunications and it has been very important to breaking cases. It has been particularly important in terrorism cases because prior knowledge is so critical, so you have got to have a prevention here.

But in the situation we are talking about here, which is information warfare and the vulnerability of the sophisticated, pervasive

information systems that we have in the United States, encryption is a form of defense. That is the question I want to ask. Is not encryption a form of defense against information warfare attack? I mean, part of it is to stop some hostile nation or terrorist group from cracking into our system, so we want encryption at that point, in that sense, to protect ourselves.

Mr. TENET. It is, Senator, a defense when it is embedded in a system. When I talked to you about the management of a key infrastructure with entities that certify your keys and you know that the transaction is valid and they know who you are, who you say you are, and they know you can send the money you sent, the authentication—in a system that captures all those features, which we are not focusing on developing because the implication is that in the absence of that system, encryption will not be widely used and we will not protect ourselves the way we need to protect ourselves.

So it is a much bigger systemic issue that we have to tackle. So we are all focused on the narrow recovery issue. Meanwhile, we are not developing products and systems that we need to protect us as fully as we possibly can be protected.

Senator LIEBERMAN. Right. And, of course, the complication is that on the other side, we would not want a hostile nation, to overuse the term, to have an encryption system that we find it impossible to gain access to because that could protect their capacity to, using more traditional military terms, launch against us.

We talk about stealth platforms, either in the air or under water. These encrypted information warfare systems, outside of the United States, are pretty much stealth platforms and in that sense, we would want to be able to figure out how to break through the encryption.

So I guess it is whose encryption and who has got the keys. But you are right, right now. What you have described today is serious, so serious and such a real threat—again, we are not here to panic people, but this is real and it is a whole new order of security threat. We ought to figure out how to get together and defend against it and set against these threats. I think the debates we are having about encryption and key access between the government and the private sector, frankly, do not seem that significant. We ought to figure out a way to overcome those debates and get something done together, to go to your word, Mr. Tenet, build trust.

Finally, General Minihan, I just want to assure you that my son has also communicated a desire for cash across the Internet, so do not feel that you are alone. [Laughter.] Thank you, Mr. Chairman.

Chairman THOMPSON. Gentlemen, thank you very much for your testimony today. We are going to have a vote any minute now, supposedly. But this has been extremely helpful. I think that you have helped to highlight this problem. You obviously are attending to it, and we will look forward to working with you to develop solutions. Thank you very much.

Mr. TENET. Thank you, Senator.

Chairman THOMPSON. We will adjourn.

[Whereupon, at 11:39 a.m., the Committee was adjourned.]

○