Testimony

Unclassified Testimony for George J. Tenet Director of Central Intelligence to be delivered to the Senate Committee on Governmental Affairs

24 June 1998

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 US 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. 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. Secondly, 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 nation - wide 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 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 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 US, they cannot prevail. These countries recognize that cyber attacks - possibly launched from outside the US - against civilian computer systems in the US - 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 US 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 infra-structure. 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.

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 cyber - space

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 US 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 US

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. More-over, 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 information 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, MD. The IOTC is another of our joint DoD and Intelligence Community activities, providing advice and developing techniques that can protect US infrastructure and systems.

- We have also actively participated in DoD War Games like the EVIDENT SURPRISE series established by US 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 US 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 Infra-structure 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 advent 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 twenty - first 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.

Return to the Main Page

footer

[Committee Members] [Subcommittees][Special Investigation]
[Jurisdiction] [Hearings] Press Releases] [Sites of Interest