Testimony

STATEMENT
of
Lieutenant General Kenneth Minihan, USAF
Director, NSA

to the

Senate Governmental Affairs Committee
Hearing on

Vulnerabilities of the National Information Infrastructure
June 24, 1998

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 21 st 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 policyrnakers, 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. policyrnakers 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. U.S. 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 21 st 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 U.S. 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 US. 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 dearly demonstrated that 10 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. Dogs 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.

Return to the Main Page

footer

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