# Chapter LII
# USA's View on World Cyber Security Issues

**Norman Schneidewind**
*Naval Postgraduate School, USA*

## ABSTRACT

*There is little evidence that the world is more secure from a major cyber attack than in 2000 because attacks on the Internet go on unabated . In addition to calling for new legislation and oversight, this chapter serves as a source of information about cyber security that domestic and international security analysts can use as a resource for understanding the critical issues and as a guide for preparing for hearings and legislative initiatives.*

## INTRODUCTION

There has been much talk by cyber security officials about plans to protect the world from cyber attacks. Unfortunately, there is little evidence that the world is more secure from a major cyber attack than in 2000 because attacks on the Internet go on unabated (see Table 1). In addition to calling for new legislation and oversight, this chapter serves as a source of information about cyber security that domestic and international security analysts can use as a resource for understanding the critical issues and as a guide for preparing for hearings and legislative initiatives. This is accomplished by describing and analyzing both the technical and policy issues. With increased understanding of the threat to the nation's cyber space, security analysts will be prepared to determine the adequacy of existing legislation and the possible need for new or amended legislation.

## MOTIVATION

Naturally, after the events of 9/11, the world focused on possible further attacks on their physical infrastructure. However, this approach is like "fighting

the last war." The enemy knows that we have gone to great lengths to protect our physical infrastructure. The probability is much higher for terrorist attacks on the nation's cyber space. Having focused on fighting the last war, we are much less prepared to protect our network resources, such as the Internet, despite the fact that a successful attack on our cyber space could bring the world's economy to its knees. In addition to security, it is important to recognize that both hardware and software reliability play a vital role in keeping the world's network infrastructure secure and operational. Therefore, the motivation of this chapter is to provide a focus on cyber security and reliability, with an emphasis on determining the extent of actual *implementation* as opposed to plans for implementation.

This chapter addresses various policy issues that have arisen in the debate on the cyber security threat in the U.S. that we believe also has significance worldwide.

## POLICY INITIATIVES FOR DEVELOPING AND IMPROVING CYBER SECURITY POLICY

There is much that can be done to enhance the security of the world's critical information infrastructure that include: (1) new thinking about how to solve the cyber security problem and (2) implementation of plans to solve the problem that have been proposed but where action has been lacking.

1. In September 2003, Microsoft Corporation announced three new critical flaws in its latest Windows operating systems software. Security experts predicted that computer hackers might possibly exploit these new vulnerabilities by releasing more attack programs, such as the "Blaster worm" that recently targeted other Windows vulnerabilities causing widespread disruption on the Internet. (Vijayan & Jaikumar, 2003)

Microsoft operating systems and application programs are notorious for having experienced numerous security breaches. Since Microsoft products account for about 90% of the installed base of software nationwide, a great deal of leverage in mitigating user vulnerabilities to attack could be gained by improving the security of Microsoft software. This factor is frequently overlooked in securing the nation's cyber space. The fact is that software vendors, such as Microsoft, *are* the most significant source of security problems. Windows operating systems and application software have been subject to repeated successful attacks for many years. Thus, making the Internet more secure is not going to solve the core problem. A possible partial solution is legislation mandating that federal government acquired software be subject to rigorous security checks by the National Institute for Standards and Technology (NIST) prior to implementation. Of course, there is a political problem in doing this: Congresspersons representing software vendors in their districts would object. However, the problem is so serious that the political risk should be accepted.

A related idea is for Congress to exercise oversight responsibility to prevent Windows operating systems from being used on mission critical government systems and to substitute a more secure system, such as Linux. Again, the political fallout that would result from implementing this idea is recognized.

The NIST would seem to be the logical organization to perform software security certification. The private sector would be required to submit its software to NIST for security certification in order to be eligible for federal IT contracts. However, if analysis revealed that it is neither interested in nor capable of performing this function, a new software certification lab could be legislated to focus on the cyber security threat. This lab would perform research and development in software cyber security in addition to certifying operational software. It is