



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003



Myra Buel

Table of Contents

Executive Summaryvii

Introduction1

Cyberspace Threats and Vulnerabilities: A Case for Action5

National Policy and Guiding Principles13

National Cyberspace Security Priorities

Priority I: A National Cyberspace Security Response System19

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program ...27

Priority III: A National Cyberspace Security Awareness and Training Program37

Priority IV: Securing Governments’ Cyberspace43

Priority V: National Security and International Cyberspace Security Cooperation49

Conclusion: The Way Forward53

Appendix: Actions and Recommendations (A/R) Summary55



Executive Summary

Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

This *National Strategy to Secure Cyberspace* is part of our overall effort to protect the Nation. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by a *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.

The *National Strategy to Secure Cyberspace* outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The *Strategy* highlights the role of public-private engagement. The document provides a framework for the contributions that we all can make to secure our parts of cyberspace. The dynamics of cyberspace will require adjustments and amendments to the *Strategy* over time.

The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all. Therefore, the *National Strategy to Secure Cyberspace* helps reduce our Nation's vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them.

Strategic Objectives

Consistent with the *National Strategy for Homeland Security*, the strategic objectives of this *National Strategy to Secure Cyberspace* are to:

- Prevent cyber attacks against America's critical infrastructures;
- Reduce national vulnerability to cyber attacks; and
- Minimize damage and recovery time from cyber attacks that do occur.

Threat and Vulnerability

Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally

designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace.

A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security. The required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date. We should not, however, be too sanguine. There have been instances where organized attackers have exploited vulnerabilities that may be indicative of more destructive capabilities.

Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities. What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving.

In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.

