# Priority V: National Security and International Cyberspace Security Cooperation

America's cyberspace is linked to that of the rest of the world. Attacks cross borders at light speed. Distinguishing between malicious activity originating from criminals, nation state actors, and terrorists in real time is difficult. This requires America to be prepared to defend critical networks and respond to attacks in each case. Systems supporting this country's critical national defense and the intelligence community must be secure, reliable, and resilient—able to withstand attack regardless of the origin of attack. America must also be prepared to respond as appropriate to attacks against its critical infrastructure. At the same time, America must be ready to lead global efforts, working with governments and industry alike, to secure cyberspace that is vital to the operation of the world's economy and markets. Global efforts require raising awareness, promoting stronger security standards, and aggressively investigating and prosecuting cybercrime.

## A. ENSURING AMERICA'S NATIONAL SECURITY

We face adversaries, including nation states and terrorists, who could launch cyber attacks or

seek to exploit our systems. In peacetime America's enemies will conduct espionage against our government, university research centers, and private companies. Activities would likely include mapping U.S. information systems, identifying key targets, lacing our infrastructure with "back doors" and other means of access. In wartime or crisis, adversaries may seek to intimidate by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. They may also attempt to slow the U.S. military response by disrupting systems of the Department of Defense (DoD), the Intelligence Community, and other government organizations as well as critical infrastructures.

America has already experienced significant national cybersecurity events. In 1998, attackers carried out a sophisticated, tightly orchestrated series of cyber intrusions into the computers of DoD, NASA, and government research labs. The intrusions were targeted against those organizations that conduct advanced technical research on national security, including atmospheric and oceanographic topics as well as aircraft and cockpit design.

The United States must have the capability to secure and defend systems and infrastructures that are deemed national security assets, and develop the capability to quickly identify the origin of malicious activity. We must improve our national security posture in cyberspace to limit the ability of adversaries to conduct espionage or pressure the United States.

1. Strengthen Counterintelligence Efforts in Cyberspace

*The FBI and intelligence community should ensure a strong counterintelligence posture to counter cyber-based intelligence collection against the United States government, and commercial and educational organizations. This effort must include a deeper understanding of the capability and intent of our adversaries to use cyberspace as a means for espionage. (A/R 5-1)*

2. Improve Attack Attribution and Prevention Capabilities

*The intelligence community, DoD, and the law enforcement agencies must improve the Nation's ability to quickly attribute the source of threatening attacks or actions to enable timely and effective response. Consistent with the National Security Strategy, these efforts will also seek to develop capabilities to prevent attacks from reaching critical systems and infrastructures. (A/R 5-2)*

3. Improve Coordination for Responding to Cyber Attacks within the United States National Security Community

*The United States must improve interagency coordination between law enforcement, national security, and defense agencies involving cyber-based attacks and espionage, ensuring that criminal matters are referred, as appropriate, among those agencies. The National Security Council and the Office of Homeland Security will lead a study to ensure that appropriate mechanisms are in place. (A/R 5-3)*

4. Reserve the Right to Respond in an Appropriate Manner

*When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies. (A/R 5-4)*

## B. INTERNATIONAL COOPERATION

The Department of State will lead federal efforts to enhance international cyberspace security cooperation. Key initiatives include:

1. Work through International Organizations and with Industry to Facilitate and to Promote a Global "Culture of Security"

America's interest in promoting global cybersecurity extends beyond our borders. Our

information infrastructure is directly linked with Canada, Mexico, Europe, Asia, and South America. The United States and world economy increasingly depend upon global markets and multinational corporations connected via information networks. The vast majority of cyber attacks originates or passes through systems abroad, crosses several borders, and requires international investigative cooperation to be stopped.

Global networks supporting critical economic and security operations must be secure and reliable. Securing global cyberspace will require international cooperation to raise awareness, increase information sharing, promote security standards, and investigate and prosecute those who engage in cybercrime. The United States is committed to working with nations to ensure the integrity of the global information networks that support critical economic and security infrastructure. We are also ready to utilize government-sponsored organizations such as the Organization of Economic Cooperation and Development (OECD), G-8, the Asia Pacific Economic Cooperation forum (APEC), and the Organization of American States (OAS), and other relevant organizations to facilitate global coordination on cybersecurity. In order to facilitate coordination with the private sector, we will also utilize such organizations as the Transatlantic Business Dialogue.

2. Develop Secure Networks

The United States will engage in cooperative efforts to solve technical, scientific, and policy-related problems to assure the integrity of information networks. We will encourage the development and adoption of international technical standards and facilitate collaboration and research among the world's best scientists and researchers. We will promote such efforts as the OECD's *Guidelines for the Security of Information Systems and Networks*, which strive to inculcate a "culture of security" across all participants in the new information society.

Because most nations' key information infrastructures reside in private hands, the United States will seek the participation of United States industry to engage foreign counterparts in a peer-to-peer dialogue, with the twin objectives of making an effective business case for cybersecurity, and explaining successful means for partnering with government on cybersecurity.

*The United States will work through appropriate international organizations and in partnership with industry to facilitate dialogue between foreign public and private sectors on information infrastructure protection and promote a global "culture of security." (A/R 5-5)*

3. Promote North American Cyberspace Security

*The United States will work with Canada and Mexico to make North America a "Safe Cyber Zone." We will expand programs to identify and secure critical common networks that underpin telecommunications, energy, transportation, banking and finance systems, emergency services, food, public health, and water systems. (A/R 5-6)*

4. Foster the Establishment of National and International Watch-and-Warning Networks to Detect and Prevent Cyber Attacks as they Emerge

*The United States will urge each nation to build on the common Y2K experience and appoint a centralized point-of-contact who can act as a liaison between domestic and global cybersecurity efforts. Establishing points of contact can greatly enhance the international coordination and resolution of cyberspace security issues. We will also encourage each nation to develop its own watch-and-warning network capable of informing government agencies, the public, and other countries about impending attacks or viruses. (A/R 5-7)*

*To facilitate real-time sharing of the threat information as it comes to light, the United States will foster the establishment of an international*

*network capable of receiving, assessing, and disseminating this information globally. Such a network can build on the capabilities of nongovernmental institutions such as the Forum of Incident Response and Security Teams. (A/R 5-8)*

*The United States will encourage regional organizations, such as the APEC, EU, and OAS, to each form or designate a committee responsible for cybersecurity. Such committees would also benefit from establishing parallel working groups with representatives from the private sector. The United States will also encourage regional organizations—such as the APEC, EU, and OAS—to establish a joint committee on cybersecurity with representatives from government and the private sector. (A/R 5-9)*

5. Encourage Other Nations to Accede to the Council of Europe Convention on Cybercrime, or to Ensure that their Laws and Procedures are at Least as Comprehensive

The United States will actively foster international cooperation in investigating and prosecuting cybercrime. The United States has signed and supports the recently concluded Council of Europe Convention on Cybercrime, which requires countries to make cyber attacks a substantive criminal offense and to adopt procedural and mutual assistance measures to better combat cybercrime across international borders.

*The United States will encourage other nations to accede to the Council of Europe Convention on Cybercrime or to ensure that their laws and procedures are at least as comprehensive. (A/R 5-10)*

Ongoing multilateral efforts, such as those in the G-8, APEC, and OECD are also important. The United States will work to implement agreed-upon recommendations and action plans that are developed in these forums. Among these initiatives, the United States in particular will urge countries to join the 24-hour, high-tech crime contact network begun within the G-8, and now expanded to the Council of Europe membership, as well as other countries.