INTERNATIONAL STRATEGY FOR CYBERSPACE

Prosperity, Security, and Openness in a Networked World

The U.S. International Strategy for Cyberspace outlines our vision for the future of cyberspace, and sets an agenda for partnering with other nations and peoples to realize it.

We live in a rare historical moment with an opportunity to build on cyberspace's successes and help secure its future—for the United States, and the global community.

Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies. The reach of networked technology is pervasive and global. To realize fully the benefits that networked technology promises the world, these systems must function reliably and securely. Assuring the free flow of information, the security and privacy of data, and the integrity of the interconnected networks themselves are all essential to American and global economic prosperity, security, and the promotion of universal rights.

Strategic Approach

The United States' approach to international cyberspace issues is founded on the belief that networked technologies hold immense potential for our Nation, and for the world. The United States will pursue an international cyberspace policy that stokes the innovation that drives our economy and improves lives here and abroad.

Our strategic approach builds on successes, recognizes the challenges to our national and economic security, and is always grounded by our unshakable commitments to fundamental freedoms of expression and association, privacy, and the free flow of information.

The Future We Seek

The cyberspace environment that we seek rewards innovation and empowers entrepreneurs; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security. This cyberspace is defined by four key characteristics:

- **Open** to innovation
- **Interoperable** the world over
- **Secure** enough to earn people's trust
- **Reliable** enough to support their work

To realize this vision, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law. These norms include:

- Upholding Fundamental Freedoms
- Respect for Property
- Valuing Privacy
- Protection from Crime
- Right of Self-Defense
- Global Interoperability
- Network Stability
- Reliable Access
- Multi-stakeholder Governance
- Cybersecurity Due Diligence

To realize this future, the United States will combine *diplomacy, defense*, and *development* to enhance prosperity, security, and openness so all can benefit from networked technology.

Diplomacy: Strengthening Partnerships

The United States will work to create incentives for, and build consensus around, an international environment in which states – recognizing the intrinsic value of an open, interoperable, secure, and reliable cyberspace – work together and act as responsible stakeholders. Through our international relationships and affiliations, we will seek to ensure that as many stakeholders as possible are included in this vision of cyberspace precisely because of its economic, social, political, and security benefits.

Distributed systems require unified action because no single institution, document, arrangement, or instrument could suffice in addressing the needs of our networked world. From end-users, private-sector hardware and software vendors, and Internet service providers, to regional, multilateral, and multi-stakeholder organizations – all are important in helping cyberspace meet its full potential.

Defense: Dissuading and Deterring

The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, thereby dissuading and deterring malicious actors, while reserving the right to defend these vital national assets as necessary and appropriate. The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks. For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them.

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

Development: Building Prosperity and Security

We believe the benefits of a connected world are universal. The virtues of an open, interoperable, secure, and reliable cyberspace should be more available than they are today, and as the world's leading information economy, the United States is committed to ensuring others benefit from our technical resources and expertise.

Our Nation can and will play an active role in providing the knowledge and capacity to build and secure new and existing digital systems. The United States' capacity-building assistance is envisioned as an investment, a commitment, and an important opportunity for dialogue and partnership. As countries develop a stake in cyberspace issues, we intend our dialogues to mature from capacity-building to active economic, technical, law enforcement, defense and diplomatic collaboration on issues of mutual concern.

Policy Priorities

This strategy is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action. It is also a roadmap allowing the United States Government's departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation.

The United States Government organizes its activities across seven interdependent areas of activity, each demanding collaboration within our government, with international partners, and with the private sector. Taken as a whole, they form the action lines of our strategic framework.

Economy: Promoting International Standards and Innovative, Open Markets

To ensure that cyberspace continues to serve the needs of our economies and innovators, we will:

- Sustain a free-trade environment that encourages technological innovation on accessible, globally linked networks.
- Protect intellectual property, including commercial trade secrets, from theft.
- Ensure the primacy of interoperable and secure technical standards, determined by technical experts.

Protecting Our Networks: Enhancing Security, Reliability, and Resiliency

Because strong cybersecurity is critical to national and economic security in the broadest sense, we will:

- Promote cyberspace cooperation, particularly on norms of behavior for states and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships.
- Reduce intrusions into and disruptions of U.S. networks.
- Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure.
- Improve the security of the high-tech supply chain, in consultation with industry.

Law Enforcement: Extending Collaboration and the Rule of Law

To enhance confidence in cyberspace and pursue those who would exploit online systems, we will:

- Participate fully in international cybercrime policy development.
- Harmonize cybercrime laws internationally by expanding accession to the Budapest Convention.
- Focus cybercrime laws on combating illegal activities, not restricting access to the Internet.
- Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks.

Military: Preparing for 21st Century Security Challenges

Since our commitment to defend our citizens, allies, and interests extends to wherever they might be threatened, we will:

- Recognize and adapt to the military's increasing need for reliable and secure networks.
- Build and enhance existing military alliances to confront potential threats in cyberspace.
- Expand cyberspace cooperation with allies and partners to increase collective security.

Internet Governance: Promoting Effective and Inclusive Structures

To promote Internet governance structures that effectively serve the needs of all Internet users, we will:

- Prioritize openness and innovation on the Internet.
- Preserve global network security and stability, including the domain name system (DNS).
- Promote and enhance multi-stakeholder venues for the discussion of Internet Governance issues.

International Development: Building Capacity, Security, and Prosperity

To promote the benefits of networked technology globally, enhance the reliability of our shared networks, and build the community of responsible stakeholders in cyberspace, we will:

- Provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity.
- Continually develop and regularly share international cybersecurity best practices.
- Enhance states' ability to fight cybercrime – including training for law enforcement, forensic specialists, jurists, and legislators.
- Develop relationships with policymakers to enhance technical capacity building, providing regular and ongoing contact with experts and their United States Government counterparts.

Internet Freedom: Supporting Fundamental Freedoms and Privacy

To help secure fundamental freedoms as well as privacy in cyberspace, we will:

- Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association.
- Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions.
- Encourage international cooperation for effective commercial data privacy protections.
- Ensure the end-to-end interoperability of an Internet accessible to all.

These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek.