NATIONAL CYBER STRATEGY

of the United States of America

SEPTEMBER 2018

THE WHITE HOUSE

WASHINGTON, DC

My fellow Americans:

Protecting America's national security and promoting the prosperity of the American people are my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of American life, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities. America created the Internet and shared it with the world. Now, we must make sure to secure and preserve cyberspace for future generations.

In the last 18 months, my Administration has taken action to address cyber threats. We have sanctioned malign cyber actors. We have indicted those that committed cybercrimes. We have publicly attributed malicious activity to the adversaries responsible and released details about the tools they employed. We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing cybersecurity risks to the systems they control, while empowering them to provide adequate security. In addition, last year, I signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The work performed and reports created in response to that Executive Order laid the groundwork for this National Cyber Strategy.

With the release of this National Cyber Strategy, the United States now has its first fully articulated cyber strategy in 15 years. This strategy explains how my Administration will:

- Defend the homeland by protecting networks, systems, functions, and data;

- Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;

- Preserve peace and security by strengthening the ability of the United States — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes; and

- Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

The National Cyber Strategy demonstrates my commitment to strengthening America's cybersecurity capabilities and securing America from cyber threats. It is a call to action for all Americans and our great companies to take the necessary steps to enhance our national cybersecurity. We will continue to lead the world in securing a prosperous cyber future.

Sincerely,

President Donald J. Trump

The White House
September 2018

Table of Contents

Introduction

America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace. Critical infrastructure, national defense, and the daily lives of Americans rely on computer-driven and interconnected information technologies. As all facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed and new threats continue to emerge. Building on the National Security Strategy and the Administration's progress over its first 18 months, the National Cyber Strategy outlines how the United States will ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity.

How Did We Get Here?

The rise of the Internet and the growing centrality of cyberspace to all facets of the modern world corresponded with the rise of the United States as the world's lone superpower. For the past quarter century, the ingenuity of the American people drove the evolution of cyberspace, and in turn, cyberspace has become fundamental to American wealth creation and innovation. Cyberspace is an inseparable component of America's financial, social, government, and political life. Meanwhile, Americans sometimes took for granted that the supremacy of the United States in the cyber domain would remain unchallenged, and that America's vision for an open, interoperable, reliable, and secure Internet would inevitably become a reality. Americans believed the growth of the Internet would carry the universal aspirations for free expression and individual liberty around the world. Americans assumed the opportunities to expand communication, commerce, and free exchange of ideas would be self-evident. Large parts of the world have embraced America's vision of a shared and open cyberspace for the mutual benefit of all.

Our competitors and adversaries, however, have taken an opposite approach. They benefit from the open Internet, while constricting and controlling their own people's access to it, and actively undermine the principles of an open Internet in international forums. They hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world. They view cyberspace as an arena where the United States' overwhelming military, economic, and political power could be neutralized and where the United States and its allies and partners are vulnerable.

Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft. Non-state actors — including terrorists and criminals — exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states. Public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities. Entities across the United States have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data as well as detecting, responding to, and recovering from incidents.

> "We will continue to lead the world in securing a prosperous cyber future."
>
> DONALD J. TRUMP
> SEPTEMBER 2018

The Way Forward

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive. Securing cyberspace is fundamental to our strategy and requires technical advancements and administrative efficiency across the Federal Government and the private sector. The Administration also recognizes that a purely technocratic approach to cyberspace is insufficient to address the nature of the new problems we confront. The United States must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation.

The Administration is already taking action to aggressively address these threats and adjust to new realities. The United States has sanctioned malign cyber actors and indicted those that have committed cybercrimes. We have publicly attributed malicious activity to the responsible adversaries and released details of the tools and infrastructure they employed. We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing the cybersecurity risks to systems they control, while empowering them to provide adequate security.

The Administration's approach to cyberspace is anchored by enduring American values, such as the belief in the power of individual liberty, free expression, free markets, and privacy. We retain our commitment to the promise of an open, interoperable, reliable, and secure Internet to strengthen and extend our values and protect and ensure economic security for American workers and companies. The future we desire will not come without a renewed American commitment to advance our interests across cyberspace.

The Administration recognizes that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks. Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains. These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes. We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war. These adversaries are continually developing new and more effective cyber weapons.

This National Cyber Strategy outlines how we will (1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability — in concert with allies and partners — to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

The Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents; destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives.

The articulation of the National Cyber Strategy is organized according to the pillars of the National Security Strategy. The National Security Council staff will coordinate with departments, agencies, and the Office of Management and Budget (OMB) on an appropriate resource plan to implement this Strategy. Departments and agencies will execute their missions informed by the following strategic guidance.