Statement for Record

"Seizing Opportunity While Managing Risk in the Digital Age"

Michael McConnell

Introduction

Mr. Chairman, Members of the Committee,

Thank you for the opportunity to speak to the Committee on Commerce, Science and Transportation today.

First, I want to open with a simple statement:

If we were in a cyberwar today, the United States would lose.

This is not because we do not have talented people or cutting edge technology; it is because we are simply the most dependent and the most vulnerable. It is also because we have not made the national commitment to understanding and securing cyberspace. While we are making progress

- the President's cyberspace policy review completed last May,
- the appointment of the Cybersecurity Coordinator in December, and
- recent investments in the Comprehensive National Cybersecurity Initiative (CNCI) are moves in the right direction but
- these moves are not enough.

The federal government will spend more each year on missile defense than it does on Cybersecurity, despite the fact that we are attacked thousands of times each day in cyberspace and we are vulnerable to attacks of strategic significance, i.e., attacks that could destroy the global financial system and compromise the future and prosperity of our nation. Securing cyberspace will require a more robust commitment in terms of leadership, policies, legislation, and resources than has been evident in the past.

Seizing Opportunity...

The cyber revolution has transformed our economy, enriched our society, and enhanced our national security. The Information and Communications Technology (ICT) sector contributes over $1 trillion to our economy each year; "smart" electric grids promise to transform our energy system; intelligent transportation systems are altering the way we move and the way we manage commerce; electronic medical records and

telemedicine promise to reduce costs while improving quality. The global financial sector relies on information technology to process and clear transactions on the order trillions of dollars each day. To put that in perspective, while the US total GDP was just over $14T last year, two banks in New York move over $7T per day in transactions.

Meanwhile, major investments in broadband – by both the government and private sector – empowers small businesses and our citizens; digital classrooms are changing the way our children are educated; and "open government" initiatives make government data more accessible and useable for business and individuals alike. Our military and security services have benefited as well. The Department of Defense has aggressively adopted network-centric operations, linking sensors, commanders and operators in near-real time and providing the U.S. a decisive advantage in the battlespace. The intelligence community and homeland security have benefited from cyber technologies by improving collaboration and information sharing across formerly impenetrable organizational divides. In short, the microprocessor and internet have been as transformative as the steam engine and railroads in the 19th century and as impactful as the internal combustion engine and interstate highway system in the 20th century.

...Managing Risk

The reach and impact of cyberspace will accelerate over the next 10 years, as another billion users in China, India, Brazil, Russia, Indonesia and Middle East gain access to the internet. As a consequence, cyberspace will be much more diverse, distributed, and complex. As cyberspace becomes more critical to the day-to-day functioning of business, society and government, the potential damage from cyber attacks, system failures and data breaches will be more severe.

In the early stages of cyberspace, the threat largely originated from "hackers" who wanted to their test skills and demonstrate their technical prowess. Criminal elements followed, resulting in attacks against financial institutions, credit card accounts, ATMs for personal gain. More sophisticated actors emerged as state-based intelligence and security organizations developed robust exploitation and attack capabilities as part of a larger national security strategy.

Recently, "hactivists" – non-state actors mobilized in support of a particular issue or motivated by patriotic reasons - have entered the fray. Generally speaking, we know and understand these threats – their capabilities and intentions.

However, of particular concern is the rise of non-state actors who are motivated not by greed or a cause, but by those with a different world view who wish to destroy the information infrastructure which powers much of the modern world – the electric grid, the global financial system, the electronic health care records, the transportation networks.

Of increasing concern is that the sophistication of cyber attack tools continues to increase at cyber speed, while the barriers to entry continues to fall as attack tools proliferate in chat rooms, homepages, and websites. The challenges we face are significant and will only grow; our response must equally bold and decisive.

Recommendations for Cybersecurity

Despite the complex and seemingly unprecedented nature of the challenge, there are some immediate actions we can take to secure cyberspace and the future of our nation.

Cyber Policy – The U.S. needs a long-term cyberspace strategy that spells our specific goals and objectives and clarifies roles and responsibilities across the federal government. This should be preceded by a cyber equivalent to President's Eisenhower's "Project Solarium" in the early 1950's in developing the nation's nuclear deterrence policy. Today, we need a full and open discourse with a diverse group – business, civil society, and government - on the challenges we face in cyberspace. This dialogue should result in a strategic framework that will guide our investments and shape our policies, both domestically and internationally.

We need a national strategy for cyber that matches our national strategy that guided us during the Cold War, when the Soviet Union and nuclear weapons posed an existential threat to the United States and its allies. Cyber has become so important to the lives of our citizens and the functioning of our economy that gone are the days when Silicon Valley could say "hands off" to a Government role. To offer historical perspective on how the government's role has increased in every case as emerging technologies effect the nation and greater numbers of our citizens, I am attaching to this statement a review conducted by my colleagues and I entitled "The Road to Cyberpower".

Cyber Operations - The Cybersecurity challenge to the nation today mirrors our response to counter terrorism after 9-11 – a host of federal and state and local agencies, each with their own authorities, missions, operations centers and information systems. The risk is that we fail to learn the lessons around counterterrorism information sharing and operations and create more silos by individual agencies, potentially creating an atmosphere of bureaucratic rivalry and duplicative investments. To that end, the U.S. should establish a National Cybersecurity Center, modeled on the interagency National Counter Terrorism Center (NCTC), that integrates elements of DoD's proposed Cyber Command, DHS's National Cybersecurity and Communications Integration Center (NCCIC), FBI's cyber operations, state and local government, and the private sector. This center should operate at the highest levels of classification for all members and serve as the hub of information sharing and integration, situational awareness and analysis, coordination and collaboration. Only sharing information across all sectors will

we be able to provide incident response across all domains of cyberspace - .gov, .mil, and .com.

Such a center would utilize the legal authorities of each agency while protecting privacy and civil liberties with appropriate oversight by the Attorney General and the Congress. The center also could serve as the information sharing and collaboration hub with our allies and other Cybersecurity organizations, providing a single conduit for outside entities.

Cyber Technology - The U.S. risks being left behind in Cybersecurity technology. Currently, multiple organizations within the government and private sector are focused on developing new technologies to protect our networks, computer systems, data and applications. However, most of the efforts are fragmented and sub-scale. The U.S. should approach this challenge as we successfully addressed to the challenge to our semiconductor industry in the 1980s through a public-private partnership focused on Cybersecurity technologies.

The U.S. should establish a Cybersecurity Collaborative Consortia, modeled after SEMATECH, a public-private partnership that supports basic research and development and develops foundational technologies and techniques of common concern – identity and access management, secure networks, intrusion detection, dynamic defense, etc. Such an organization should work closely with the National Institute of Standards and Technology (NIST) and with the National Security Agency (NSA) to define standards for Cybersecurity that could be used for government, business, and individuals in both the public and private sectors because there are no effective boundaries in cyber space.

Cyber Human Capital – The U.S. needs a Cyber Education and Training Initiative (akin to the National Defense Education Act of 1958 after the launch of Sputnik) to build our national human capital base in math, science and technology, electrical engineering, computer science, and cybersecurity. Recent initiatives by Congress in programs like the Federal Cybersecurity Scholarship for Service and the Information Assurance Scholarship Program are a start, but need to be more aggressively funded to build the expertise we need in cyberspace. As a country, our vulnerabilities will only grow without a highly trained workforce than can respond to the daunting cyber challenges and opportunities of the 21st century.

Cyber Management – Current spending and oversight on Cyber is spread among multiple accounts and dispersed over multiple committees in Congress. It is difficult to understand the current level of investment in cyber and evaluate the effectiveness of

our investments given this complexity and lack of transparency. OMB, working with Congress, should identify Cybersecurity investments, develop performance criteria aligned against a national cyber strategy, address the gaps and eliminate duplicative or conflicting efforts, and improve accountability for results. We can not spend our way out of this challenge;, prioritization, accountability, management and oversight are key.

Summary

Cyber technologies offer unprecedented opportunities for the nation; however, they also present significant risks to our infrastructure, our financial systems, and our way of life. We prevailed in the Cold War through strong leadership, clear policies, strong alliances, and close integration of all elements of national power – economic, military, and diplomatic – supported by a bi-partisan, national consensus around containment and deterrence. We must do the same with Cybersecurity.