

National Strategy Forum Event Summary: Stewart Baker & Cyber Security

By Eric S. Morse

On Monday, October 5, 2009, Stewart Baker, former Assistant Secretary for Policy at the Department of Homeland Security, addressed the National Strategy Forum on the topic of cyber security and the risks to America's virtual reality.

Every day, millions of Americans log onto their computers for personal use. We check our email, manage our finances, send important corporate documents, and view other media without giving much thought to the complexities behind these seemingly normal tasks. Moreover, we rarely wonder, behind the false veil of anonymity and security of our computer screens, who else might be snooping around in the background of the browser window.

Stewart Baker argues that America is more vulnerable to cyber-related attacks than private citizens and government officials realize. For many years, computer technology has grown at an exponential rate. Twenty years ago, it was inconceivable that IBM would be able to put a computer in every home. Today, young children arrive at school with the equivalent of a supercomputer in their pockets. Technology has exploded, filling nearly every corner of our lives. At the same time, cyber security significantly lags behind.

Cyberspace and computer technology is vulnerable to both state and non-state actors. Individual hackers can create computer viruses, codes, or programs that steal information from another computer that can be used for profit or worse. State actors, such as China and Russia, have the capability of unleashing massive barrages of computer attacks on U.S. defense networks, utility sectors, financial institutions, government servers, and other important national infrastructures. Yet despite these evident threats, very little has been done to increase America's cyber security. Why is this the case?

The government has been working for a decade or more on solutions to cyber threats. However, a litany of barriers prevents productive policy solutions.

First, government policymakers face unpopular policy options. The government is unwilling to push the limits of personal privacy in order to take the necessary steps to ensure online security. For cyber security to work, previous definitions of privacy and civil liberties may need to bend to accommodate the solutions that could make us safer. This is a tenuous line to walk—our way of life, both online and ethically, may need to change.

Second, private and public investment in cyber security is very expensive. In order to provide the necessary security measures, vast swaths of the technology industry would need to be altered to improve security. These costs are difficult to overcome initially.

Private individuals and public policy makers find it difficult to justify large financial expenditures for a threat that is not yet fully realized.

Third, the difficulty of identifying the perpetrators is a prominent challenge to creating effective responses to cyber attacks. So far, many cyber attacks are accomplished with near-complete anonymity. Both the public and private sectors need improved tools for identifying the origin of cyber attacks before the appropriate responses can be implemented.

Fourth, a government vacancy remains in the department of cyber security: there is no “Cyber Czar” in charge of protecting America. This vacancy is partly due to the serious challenge facing any potential candidate. No one wants to be held responsible for inevitable cyber attacks if there are no current solutions to the problem. That would be political and career suicide. This lack of political leadership leads to a lag in government-level policy coordination.

All of these policy options are fraught with added expense, political risks, and personal privacy concerns. Despite these challenges, doing nothing will certainly lead to greater vulnerability and attacks with unknown national consequences. America needs to get serious about pursuing cyber security before it is too late.