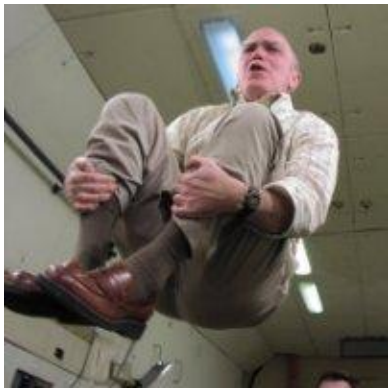
CyberPro

February 2011

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: STEWART BAKER



*NSCI's Charles Winstead recently had the opportunity to interview Stewart Baker, former Assistant Secretary for Policy at the Department of Homeland Security and General Counsel of the National Security Agency. Stewart A. Baker is a partner in the Washington office of Steptoe & Johnson LLP. He returned to the firm following three and a half years at the Department of Homeland Security as its first Assistant Secretary for Policy. He's written a book about terrorism, technology, and his time at the Department, entitled "**Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism.**" He devotes about a third of the book to cybersecurity.*

At Homeland Security, Mr. Baker created and staffed the 250-person DHS Policy Directorate. He was responsible for policy analysis across the Department, as well as for the Department's international affairs, strategic planning and relationships with law enforcement and public advisory committees. This work required a broad understanding of all aspects of the Department's activities, including maritime regulation, customs enforcement, immigration, identity management, SAFETY Act implementation, money laundering enforcement, government contracts, and regulation of travel and air transportation, and its role in the Committee on Foreign Investment in the United States ("CFIUS"). While at DHS, Mr. Baker led successful negotiations with European and Middle Eastern governments over travel data, privacy, visa waiver and related issues. He devised a new approach to visa-free travel, forged a congressional and interagency consensus on the plan and negotiated acceptance with key governments. He also managed the passage and implementation of the SAFE Ports Act, led the Department's policy effort to reform federal immigration laws, and transformed the Department's role in CFIUS, helping to drive the first rewrite of the CFIUS law and regulations in a generation.

NSCI: In early 2010 you participated in the Bipartisan Policy Center's Cyber Shockwave. What were your key takeaways from that simulation and what progress do you think has been made since the simulation?

BAKER: I was struck by how uncertain everyone was about the government's authority to take action in response to the crisis. Some very senior former officials had grave doubts about their ability to take actions that were quite reasonable in the circumstances. For example, it made sense in the context of the facts we were given to keep infected machines off the Internet, yet it was not clear that the government could order ISPs to do that, despite the enormous harm being caused by the infected machines.

I don't see as much change as I'd like in that basic attitude. The Justice Department doesn't seem to be in problem-solving mode. Instead, I get the sense that the Justice lawyers are in problem-finding mode.

The good news is that the lack of certainty dramatized by the event may have been partially responsible for the strong interest being shown by Congress in cybersecurity legislation that would spell out the government's emergency authorities.

NSCI: What positive steps have you seen the current administration take to secure cyberspace? Where should they focus their efforts to get the most bang for the buck over the next two years?

BAKER: The President started out well, saying even in the campaign that this would be one of his top national security priorities, giving the first Presidential speech devoted to the issue, and ordering a plan very soon after inauguration. Since then, though, there's been a lot of drift and disarray on the issue.

We're letting the lawyers set the pace and the direction. Speaking as a lawyer, and someone who loves the law, that is a recipe for failure. Government lawyers in particular need direction from policy makers, and I don't think they're getting enough.

NSCI: How do you think we are doing in implementing the recommendations from the "Hathaway Report"?

BAKER: The Hathaway Report kicked the can on the hard issues. In many ways, the report was almost embarrassingly similar to the 2003 Bush Administration report on the same topic, which also kicked the can on the hard issues. The Hathaway report promised that the appointment of a cybersecurity coordinator would kick off a process that finally addressed these issues. We've got a cybersecurity coordinator in the White House, but he's found what Melissa found – there are too many competing power centers in the White House and elsewhere to make rapid progress. Only the President can break the deadlock. I don't know if he's ready to do that.

NSCI: Congress has introduced numerous bills related to cybersecurity. What are some of the key challenges you think these, and future, bills should be tackling?

BAKER: This is an area where there's clearly been a market failure – the same kind of market failure you'd expect if we told Ford Motor executives that they are responsible for their own air defense in the event of an attack. Some kind of government intervention is needed, and usually you'd expect that to take the form of regulation. The difficulty is that regulations move much more slowly than the threat. The challenge is to find a way to incentivize the private sector to adopt effective, imaginative, and immediate changes in their security posture – over and over again. That's not how the regulatory process usually works, so real creativity is going to be necessary.

NSCI: What actions would you like to see regarding cybersecurity national policy, authorities, roles, and responsibilities?

BAKER: The law creating DHS gave that agency responsibility for most cybersecurity issues in the civilian sector. But for years DHS was largely incapable of carrying out its responsibilities. That has changed over the last few years, and DHS is now a little better than its reputation. Rather than opening a battle over turf, I would reaffirm DHS's role, while also encouraging other agencies, such as the National Security Agency and the Commerce Department, to use their security authorities in a complementary fashion.

NSCI: What key cybersecurity threats and/or vulnerabilities do you think we need to address with a sense of urgency as opposed to what is less important given we can't do it all at once?

BAKER: Most experts in the field think that consistently keeping bad guys out of networks is not feasible. Getting in is just too easy. But our security systems are still focused on policing the borders – instead of tracking what's happening inside our networks. Witness Bradley Manning, who downloaded gigabytes of information from all over the SIPRNet without anyone asking why. So one urgent task is to fire the people who failed to install audit capabilities on the systems Manning exploited, and then to install much better mechanisms for tracking users inside government systems and identifying anomalies in their activities – without letting the agencies retreat behind organizational lines and return to information-hoarding.

NSCI: What should be done to improve information sharing between government and industry regarding cyber threats, vulnerabilities, and risks?

BAKER: Industry will share information with government only if it sees value in the sharing. Thus, DHS needs to be a conduit to expertise that industry values, or it needs to have sufficient regulatory clout that industry shares information just to show DHS that it is acting responsibly.

NSCI: How do you think The National Strategy for Trusted Identities in Cyberspace (NSTIC) will help with the challenges of attribution in cyberspace? Are there any "next steps" you'd like to see us take to further help with attribution?

BAKER: Better authentication is a critical part of improving security; the Obama Administration deserves credit for seeing that, and for trying to do something about it. That said, I think the Administration was determined to produce a policy that would win at least grudging praise from privacy groups, so they loaded the initiative with a lot of unrealistic technical requirements and limitations that seem to have mollified some privacy groups but that I suspect will make the strategy unsuccessful.

NSCI: Finally, do you have any thoughts on how we handle the privacy and civil liberty concerns regarding cybersecurity?

BAKER: I spent a lot of time on this in *Skating on Stilts*. Privacy and civil liberties are important, and we all want to protect them, but an undue focus on these issues has hurt us badly, and will hurt us worse in the near future.

Privacy and civil liberties advocates spent ten years thinking up reasons why improving cybersecurity wasn't a good idea. They killed the Clinton Administration's cybersecurity drive in 1999. Then they killed the Bush Administration's cybersecurity drive in 2003. Now they're hobbling the Obama Administration's cybersecurity drive.

We've spent more than ten years being told that giving government more authority to improve network security will lead to 1984. Now, thanks to the privacy advocates' stalling, and the resulting dramatic loss of computer security, we already live in a world where authoritarian governments do use the screens and cameras in our homes and offices to watch us, listen to us, and even monitor our thoughts as we type private correspondence. All of that happened to the Dalai Lama's workers, and to workers all around the world – at Associated Press, Deloitte and Touche, Indian embassies. It's the full 1984 experience, except that we're paying for the screens and cameras. That, and the authoritarians that watch us aren't located in the United States. That's the legacy of the privacy groups on this issue.

NSCI: Thank you very much for taking the time to visit with us.