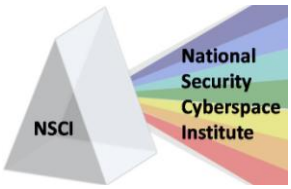

Cybersecurity: Improving the White House Grade

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

Introduction

Back in January, NSCI released a report, entitled "Federal Government Cybersecurity Progress: Obama Administration Report Card, 2009-Present," as an evaluation of how well we thought the administration has done when measured against the Near-Term Action Plan contained in the "Hathaway Report," a cyber policy review approved and released by the President in May 2009. Since that time much discussion has passed, and again without much progress. In fact, despite continuing reckless, anti-social, and criminal behavior on the net, the *National Journal* reported that President Obama's Cyber Czar, tasked with coordinating the country's response to cyber threats, said that the risk of such attacks is often overblown.[1] Howard Schmidt, the White House cybersecurity coordinator, told *National Journal* that a few sensational events make the overall cyber threat seem worse than it really is. "It's still a situation where specific incidents make it something it's not," he said. "Things make headlines that are just the risk of doing business in many cases." As a counterpoint, the Department of Commerce has detailed that about 8.1 million U.S. residents were victims of ID theft in 2010. The cost to business is high: A company with 500 employees spends about $110,000 a year just managing employee IDs, and that is clearly apart from what gets stolen or corrupted. And what about another "cost of doing business" example? According to a report by CyberFactors, the e-mail services firm Epsilon is likely to spend up to $225 million in total costs as a result of a recent data breach in its cloud computing systems. The ripple effect from this breach may have affected 75 of Epsilon's customer companies and could eventually cost these companies an additional $412 million. Further, by the time the dust finally settles on all the forensic audits, fines, litigation and lost business for provider and customers, the total tab could eventually run as high as $3 billion to $4 billion.[2]

When framed in the recently updated significant Cyber events since 2006 we think that shrugging and looking at the problem as "… just the cost of doing business" is exactly the wrong approach. With the heralded upcoming release of Congressional, Agency, and DoD Cyber organizational, policy, and strategies we felt that laying out a framework for comparison of what might be done and what apparently is finally going to be done would be useful. This may serve as a useful point of departure to start thinking about what the metrics of progress might be beyond the rumored, and much anticipated, announcements in the not too distant future.

Two areas in our Report Card – development of an updated national strategy and initiation of a national awareness campaign – particularly seemed to be lynch pins of "getting off the dime." We awarded grades of "D" and "B," respectively, to those two action items from the Hathaway Report. It was our belief that a comprehensive strategy, with all its constituent elements, would provide the guidance and priorities necessary for government agencies – from federal departments to states, counties, and municipalities – to develop operational- and tactical-level plans and programs, while performing a similar function for private sector partners… and that was most clearly missing. Additionally, at the other "end" of the problem, an aggressive national awareness and education campaign would serve to not only enhance security all the way down to the individual, casual Internet user by educating and promoting personal responsibility, but long-term would also prove instrumental in building our current and future workforce of cyber professionals who are so crucial to our success. Admittedly, nothing is impossible for the man who doesn't have to do it… so in this review, we would like to flesh out what might be done to address the policy and roadmap gaps that we believe exposes us to a growing threat.

As demonstrated by our January grade, we believe the administration is doing a creditable job expanding on the awareness and education efforts first implemented by the Bush administration's Comprehensive

[1] "White House Official: Cyber attacks are risk of doing business," National Journal, Josh Smith, 27 April 2011, available at http://www.nextgov.com/nextgov/ng_20110427_6375.php

[2] "Total cost of Epsilon breach could reach $4 billion," Help Net Security website, 2 May 2011, available at http://www.net-security.org/secworld.php?id=10966

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

National Cybersecurity Initiative (CNCI). Setting in motion a variety of programs, the federal government has not only attempted to increase awareness within the public sector, but has also mobilized industry and academia to implement even more programs to improve cybersecurity awareness. Appendix 1 shows a list of some of those programs. Interest in these is growing; participation levels are increasing, and new programs continue to spring up across virtually all sectors of the country. In spite of these success stories, however, gaps still remain, primarily in educating the general public on the dangers of poor hygiene on the net and in the small business community.

The "general public" audience we mention above refers to the everyday, non-technical Internet user. These are people who routinely use the Internet, but don't consistently keep up with the cybersecurity threats, vulnerabilities, and risks. It's not that they don't want to do their part to help with cybersecurity; they just aren't exposed to the do's and don'ts on a routine basis and either don't know how to or have decided not to install and maintain proper security tools.[3] National, state, and municipal efforts should be initiated to provide these individuals, the vast majority of Internet users, the cybersecurity education and awareness they need to be a part of the solution and secure their computers and personal information.

With regards to K-12 cybersecurity education and awareness, our research shows that information and resources are not lacking. In fact, quite the opposite is true. As shown in Appendix 2, numerous organizations have produced education and awareness material aimed at this audience. However, many K-12 educators are simply not aware of the cybersecurity risks to this age group or the material that is available to them. Further, they are often not required to include cybersecurity in their curriculum. As a result, increased focus is needed on putting the available information to use.

After recounting all of that, we are convinced cybersecurity education and awareness is reaching a point of diminishing returns. Certainly, additional cyber professionals are needed, and endpoint security should be improved. But increased manning, better training, and endpoint security will only do so much to help defend our networks and information absent some higher-order decisions.

Because small businesses play such an important role in the economy, it is imperative that they be key participants in our nation's cybersecurity efforts. According to the Small Business Administration, small businesses employ over half of all private sector workers and have generated nearly two-thirds of all net new jobs during the past 15 years.[4] Small businesses are also great innovators. As stated by Roy Rosin, vice president of innovation at Intuit, "Innovation isn't restricted to science labs and corporations. It's the driving force behind small business entrepreneurship. Small businesses instinctively use innovation to create new products and services, efficiently manage their business or find and acquire customers. These innovations are the keys to their future."[5]

To understand the importance the U.S. assigns to small business innovation, one need only look at the federal Small Business Innovation Research (SBIR) program. Over $2.5 billion is provided annually to small businesses for innovation research – an amount that reflects only a portion of the total spent by small businesses in this area.

With this emphasis on innovation, small businesses are increasingly priority targets for cyber espionage. And with limited resources available for security, these businesses are often easy prey and risk paying a

[3] A study by the National Cyber Security Alliance found that 77 percent of 326 adults in 12 states assured researchers in a telephone poll they were safe from online threats. When experts visited those people to examine computers, they found two-thirds of adults using antivirus software that was not updated in at least seven days. Two-thirds of the computer users also were not using any type of protective firewall program, and spyware was found on the computers of 80 percent of those in the study… true, even properly configured tools are no panacea, but at least it is a start.

[4] U.S. Small Business Administration website, Frequently Asked Questions, available at http://www.sba.gov/advocacy/7495/8420

[5] Intuit Study: Small Businesses Will Innovate Today to Succeed Tomorrow, Press release, 16 Mar 2009 available at http://about.intuit.com/about_intuit/press_room/press_release/articles/2009/SmallBusinessesInnovateToday.html

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

heavy price when data breaches occur. It has been estimated that since 2005, approximately 100 million breached records have been from retailers, merchants, and other types of non-financial, non-insurance companies. The majority of these businesses are small to mid-sized, with cyber attacks directed against them resulting in stolen information such as credit card, social security, and customer account numbers. When records are compromised, the results can be devastating. Not only does the surrounding negative publicity affect a company's bottom line, but at a cost of over $200 per compromised record, the financial losses to a small business are often impossible to overcome. According to John Sileo, a professional identity theft consultant, 80 percent of small businesses that experience a data breach go bankrupt or suffer severe financial losses within two years of the attack.[6] In addition, according to Javelin's 2011 Small Business Owners Identity Fraud Report, cybercrime targeted at small and medium size businesses totaled more than $8 billion in 2010.

Given the low price and relative success of cyber espionage, why wouldn't nations attempt to steal the information rather than investing the billions of dollars it would otherwise cost? Small businesses simply do not have the money or personnel to employ large cyber staffs focused on securing their networks and information.

However, the bottom line is that many people (correctly, we think) have recently opined that cybersecurity defense as a whole is probably not perfectible; we will never have a 100% secure Internet. Nevertheless, we must have the capability to operate through successful intrusions, "cauterize," enclave, or quarantine networks as a matter of policy, recover or rebuild data that is stolen or corrupted, and have mechanisms, policy, and the will to identify, arrest, and prosecute those who commit these crimes. While continuing our education, awareness, and defense efforts, we must finally end the lip service and step up to make some tough cybersecurity policy and strategy decisions we have thus far been unwilling to make. We offer below some recommendations on a few issues we believe are must-do's for the federal government.

In developing strategy, policies, and plans, we first need to decide what we want to do. Simply saying we want a "more secure cyberspace" makes for a nice PowerPoint banner at this week's cyber symposium, but hardly serves any purpose beyond that. Next, we need to ensure we have the technical ability to do what we want to do… this is a policy killer… if the wonks aren't convinced "you can do it," they will never do the hard work to make sure you CAN do it… and the circle goes 'round and 'round.

Then, we need to frame the regulation or law to support what we want to do and can technically do. Though framed as sequential, the best approach is parallel… time is wasting!
Finally, we need to move ahead and produce. An 80% solution is better than none, which is what we have now. Make someONE responsible, give them the support, the authority, and the money… and "just do it"... write it with a codicil to be reviewed by date certain…. soon. Later, policy should be allowed to change as the world changes and we get smarter. Let's not get mired down yet with what might happen in 2030, let's fix 2012 and adjust on the back nine.

Okay step one, what do we want to be able to do? Let's look at some of the issues.

Prime Issue number one...Who's in charge?

Who can say "yes" or "no", and make it stick? Right now there is no one. As we've learned over the past two-plus years with any number of issues, the president is a world-class delegator and vacillator. He waited seven months to appoint a Cyberspace Coordinator, during which time the position's authority was allowed to become so diluted that Howard Schmidt has become almost irrelevant. Schmidt has virtually

[6] 15 "Data Security Tips to Protect Your Small Business," Jennifer Schiff, *Small Business Computing*, 19 October 2010, available at http://www.smallbusinesscomputing.com/webmaster/article.php/3908811/15-Data-Security-Tips-to-Protect-Your-Small-Business.htm

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

no money, certainly no authority, and has been reduced to going around town to symposia and bemoaning the fact that others are using the term “Cyber War” to describe the current state of affairs. Not to mention his latest comment that cyber crime is just the cost of doing business.[7] It is time to suck it up and pay the piper. It seems the administration believes that by simply changing our terminology – Overseas Contingency Operation, Man-Caused Disaster, and Kinetic Military Action, for examples – we can alter the actions and attitudes of enemies, criminals, and crazies. This technique doesn't seem to be working; perhaps the president should consider adding some teeth to his cyber coordinator's authority.

Roles and responsibilities throughout the government continue to be muddled. The Department of Homeland Security (DHS) has the rose for Critical Infrastructure Protection (CIP), but clearly does not have the organic talent the National Security Agency (NSA), United States Cyber Command (USCYBERCOM), the military services, and several agencies do. The Federal Communications Commission (CC) clearly “regulates” communications, but is bogged down in an etymological swamp over what constitutes communications and what is “net neutrality.” Meanwhile, Congress claims oversight but has variously tried to promulgate over 85 bills over the last few years to energize, regulate, or circumscribe “Cyberspace,” most of which are uncoordinated, long-term, ill-defined or myopically narrow “one-off” stabs at fixing “something” with no cohesive administration counterpoint to provide a comprehensive strategy. In the final balance, beyond NSA or USCYBERCOM – who are the obvious technical picks, but the equally obvious non-starters – it really doesn’t matter who is in charge. The president has to exhibit some real leadership, make the pick, and then back the pick. Whoever is in charge doesn’t need to be able to do it all, they just need the authority to coordinate it all and set up the lanes in the road, as in, “You do this, and you do that, and both of you do it according to this roadmap and make sure it integrates with each other. If you disagree, come to me; I will make the call. And if you don’t like it, our next stop is the President.” As an example: When you fly, it doesn’t really matter if you are a crop-duster, a business tycoon, a load of potatoes, or someone breaking into the mile-high club; you fall under the rules of the Federal Aviation Authority (FAA) as you move through the medium of air, whether in a balloon, a sail-plane, a 747, an F-22 Raptor or Snoopy’s blimp. The FAA owns flying; who owns “Internetting”?

Prime Issue number two… WHAT’s important… or not?

While pretending that someone actually is in charge and is driving the boat, let’s parse out a few more issues recently in the spotlight and sparking a fair amount of debate.

Let's start with Network Neutrality

Net Neutrality generally means that Internet service providers may not discriminate between different kinds of content and applications online. Proponents maintain it guarantees a level playing field for all websites and Internet technologies. As the discussion becomes more strident, Net Neutrality is flogged as the reason the Internet has driven economic innovation, democratic participation and free speech online. Proponents claim it protects the consumer's right to use any equipment, content, application, or service without interference from the network provider. With Net Neutrality, the network's only job is to move data – not to choose which data to privilege with higher quality service. On the other hand, users have always been able to pay for higher quality service – from 56K dialup, to cable/satellite, to T-1 lines – getting more bandwidth and speed for more money. Somehow, potential net neutrality legislation and regulation appear to conflate non-discrimination with a ban on access tiering. The core issue is not whether speeding up one website over another is discriminatory; it is whether without regulation service providers will engage in monopolistic and unfair practices to limit access (some say ‘cripple’) competitors for software or devices. While we find the subject of Net Neutrality to be interesting and important, we

[7] "White House Official: Cyber attacks are risk of doing business," National Journal, Josh Smith, 27 April 2011, available at http://www.nextgov.com/nextgov/ng_20110427_6375.php

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

don't believe it to be a core cybersecurity issue. Its outcome will not inherently make cyberspace more or less safe and secure. Decouple it, give it to someone besides the Cyber Czar, and move on.

The next swamp is the Communications Assistance for Law Enforcement Act (CALEA) of 1994.

CALEA's purpose is to enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure they have built-in surveillance capabilities, allowing federal agencies to monitor all telephone, broadband Internet, and VoIP traffic in real-time. The U.S. Congress passed the CALEA to aid law enforcement in its effort to conduct criminal investigations requiring wiretapping of digital telephone networks. CALEA obliges telecommunications companies to make it possible for law enforcement agencies to tap any phone conversations carried out over its networks, as well as making call detail records available. The Act stipulates that it must not be possible for a person to detect that his or her conversation is being monitored by the respective government agency. As the Internet has burgeoned, so have the methods of communications, whether through chat channels, encrypted gaming channels, and various others. Predictably, law enforcement has pressed for broadening of CALEA to force providers and developers to spend time and money to create “backdoors” that can expeditiously provide access for court-approved surveillance. Just as predictable, privacy advocates, conspiracy theorists, and industry innovators and economists press for limiting CALEA based on a number of reasons. Once again, the survey says, “Not a core cybersecurity issue; decouple, and move on." Unless you consider your own government the enemy, the CALEA outcome will not make cyber more or less secure from criminals and others wishing to do harm and/or conduct illegal activity via cyberspace.

The point of this is that someone has to have the authority to parse things out and set priorities. Important ancillary issues, such as the two above, should not be allowed to force focus from the central important issue, which is...?

What we want to be able to do

Let’s take a wild guess and say for discussion’s sake we want the Internet to be a safe, secure, and reliable network of communications and commerce. Someone will probably quickly say, “No, we want the Internet to be safe from attack and we want people to stop attacking us through the Internet.” Well, we don’t want people to drive drunk, steal from us, and commit murder, either. But over the years we have learned to, “Don’t let friends drive drunk, look out for the other guy, crime proof ourselves and our homes.” Originally the Internet was a network designed first for hundreds and then a few thousand researchers with known identities at pretty much known locations. Now we are operating a network that has billions upon billions of users who do not know one another, should not trust one another, and, in many cases, work hard to maintain layers of anonymity. If you have ungoverned space, physical or virtual, the lawless will seek it out. What we really want to do is make an ungoverned space less dangerous and unruly.

Step one is we have to make criminal, anarchic, and adversary activity through the Internet hard, dangerous, and worthless. Willie Sutton, when asked why he robbed banks, replied in an incredulous tone, “That’s where the money is!” Similarly, if we could ask criminals, hacktivists, and adversaries why their weapon of choice is the Internet, their compiled reply would be something like, “That’s where the money, data, and advantage are; it is too easy not to try. Even if you're discovered, you probably won’t get caught!” If, on the other hand, it took them a lot of high-end talent, and they could never be sure that they weren’t being tailed or set up, and they could never be sure they weren’t stealing mines, bogus corrupted data, or the equivalent of a smallpox blanket, it would dampen some of the enthusiasm and thin out the attacking hordes.

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

So rather than hold another symposium, have an administration official say "cyber" in another speech, or concoct a science and technology program for 5th graders that, while interesting and important for the year 2025, does nothing for the sucking chest wound of 2011, what should we do?

In the words of Sun Tzu, "The art of war teaches us to rely not on the likelihood of the enemy not coming, but on our own readiness to receive him; not on the chance of him not attacking, but rather on the fact that we have made our position unassailable." Therefore, we need to put projects in place that improves the hygiene of the Internet, allows us the ability to cauterize an infection, and ensures that we can enclave the infected from the not-yet-infected. To do that we need rules – with consequences. However, as much as we would like it, this is not about reducing attacks to zero, but operating through attacks, reducing time to restoration to zero, and extending the time to "re-fix" to infinite.

How to do that *(first steps)*

1. **Harden the backbone**. Tier 1 ISPs must be looking for and reporting malware and suspicious behavior, and they must actively quarantine users who are operating outside of their contracted agreement. They often have the most reliable information regarding endpoints that become infected with viruses, malware, and other harmful software. At the user level, the ISP should be directed to notify infected users. Additionally, "power users" such as banks, the defense industry, and large commercial web companies must be on notice to defend their own enclave, up to and including disconnecting from the larger Internet on demand. To make this effective, the government must agree to support companies with critical warnings and indemnify and protect them from frivolous legal attacks. Companies with large data operations would be required to conduct off-site storage for rapid reconstitution. The focus has got to be on operating through attack when possible, cordoning off from attack when forced, and resilience in reconstitution after attack. This is not going to be easy. As an example within the government, just recently the Department of Justice (DOJ) and Federal Bureau of Investigations (FBI) took on the Coreflood botnet.[8] Federal authorities obtained an unprecedented temporary restraining order that allowed them to seize five command-and-control (C&C) servers that managed Coreflood. Since then, the U.S. Marshal's Service has operated substitute C&C servers that have disabled the bot on most infected PCs. However, in an interesting twist, in order even for the FBI to remotely uninstall the Coreflood botnet Trojan from some infected Windows PCs over the next four weeks, an additional order specified this would be permissible only when the owners have been identified by the DOJ and they have submitted an authorization form to the FBI..

2. **Secure the power grid.** When you are out of power, you are out of Schlitz. Despite more and more reports of successful clandestine activity on power grid networks, we have yet to start a program of getting the control portion of the grid out of cyberspace. Will that be inconvenient? Yes. Will it cost more to not have unimpeded remote access? Most probably. But until we understand the current secondary, cascading-failure modes and get a secure and "enclave-able" command and control arrangement, we daily face the specter of a "Pearl Harbor on steroids."

3. **Start public-private information sharing on a major scale today**. That means getting intelligence information stripped of sources and methods to companies that need it to defend their nets. That means creating the conduit to the system administrators who can actually use it – not the weekly gee-whiz briefs to CEOs who are then told to not share with anyone… or conversely the in-depth classified excerpts to the CIO or CTO that can't be shared with the uncleared CEO who has to explain to customers and shareholders. On the other side, the government has to

[8] "DOJ gets court permission to attack botnet," ComputerWorld, Grant Gross, 13 April 2011, available at http://www.computerworld.com/s/article/9215801/DOJ_gets_court_permission_to_attack_botnet

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

become the trusted clearinghouse for "commercial" or "business intelligence" information stripped of proprietary and "company identifiable" data. As Ed Amoroso, Chief Security Officer at AT&T, recently commented: "Should I share that (network security measures) information with Verizon? The answer is 'Curse word,' no, period. Let them go figure it out on their own."[9] The government must find a way to allow companies to protect their competitive advantage (solutions) while also compelling to share information regarding the attack vector itself. It does us little good after an 18-month forensic investigation to find out the attack happened twice before to three other companies 24 months ago and, for fear of consumer or stockholder backlash or loss of competitive advantage, no one mentioned it.

4. **Take initial steps to internationalizing cyber defense**. Forge a coalition of the willing around cyber crime. Just as nations are accountable for what goes on within their borders in a physical sense, the corollary is that nations have a national cyberspace accountability. When notified of a problem (presuming they have not already identified "anomalous behavior;" see #1 above), nations have an obligation to investigate, seize evidence, and prosecute hostile or criminal behavior originating within their borders. Richard Clarke's book on cyber war puts it very elegantly: "If you have an arsonist in your basement, and every night he goes out and burns down a neighbor's house, and you know this is going on, then you can't claim you aren't responsible." We ought to be able to at least sign up to that!

   We may have taken a step in the right direction recently when the U.S. and Russia collaborated on a first-ever Critical Terminology Foundations document – a guide to resolving cyber conflicts that also provides definitions of terms such as "cyber crime," "cyber war," and "cyber security."[10] Although this may seem to be a small first step, it's a good start because of the importance of a standardized terminology to the development of international agreements.

After we've incorporated the above four items into our overall cyber policy and strategy, we can attend to some of the other, more controversial issues that require resolution or, in some cases, are serving as distractions.

Additional issues and actions

Internet Kill Switch

First, there's the so-called Internet "kill switch." In our opinion, there is no such thing. We can find no evidence of a nation or group having this capability, even if there were an intent to use it. In the cases of Egypt and Libya, these authoritarian regimes were able to combine government ownership and shutdown of key cyber infrastructure with strong-arm tactics against the countries' very limited number of ISPs to achieve, at least temporarily, the effect of a kill switch. With all of the access points and resiliency built into our Internet infrastructure, we doubt that a scenario involving a widespread, prolonged outage could be achieved in the United States and other western countries. However, even in the absence of all-out disruptions, we should anticipate continued DDoS attacks, theft of financial resources, and loss of intellectual property at the hands of cyber criminals and competing nation-states. And so should by policy edict that certain industry/business entities must have the ability in extremis to disconnect themselves from the network as a contagion ensues… and have the triggers established well before the screens go dark or data disappears.

[9] " Private sector official condemns mandatory cybersecurity information sharing", Fierce Government, David Perera, 5 May 2011, available at http://www.fiercegovernmentit.com/story/private-sector-official-condemns-mandatory-cybersecurity-information-sharin/2011-05-05

[10] "U.S., Russian Officials Work to Define Cybersecurity Terms" by Christopher Brook, The Kaspersky Lab News Service, 28 April 2011, available at http://threatpost.com/en_us/blogs/us-russian-officials-work-define-cybersecurity-terms-042811

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

Internet Privacy

Another issue that continues to stir controversy is that of Internet privacy. For the foreseeable future, there will continue to be a fine balancing act between the protection of citizens' rights to privacy and providing a secure Internet. Most Americans are willing to accept some regulation in order to protect their access but are unsure of where they would draw the line in giving up some of their freedoms and privacy. Unfortunately, opinion shapers seem to modify their stance on this issue based on who is sitting in the White House. During the Bush years, the hue and cry emanating from the media over certain provisions of the Patriot Act, passed in response to the 9/11 attacks, bordered on hysteria. Much of the media has been quiet for the last two years, however, having nothing at all to say when President Obama recently signed a one-year extension – with no revisions – to that very same bill. We need to remove politics from the equation and engage in an objective debate focused on this balance, i.e., what is the minimum amount of government interference required and the maximum amount of risk we're willing to accept? We owe it to the American people to be open about this issue, including the role being played by NSA.

Trusted Identification

Closely allied (or in opposition to) Internet privacy is the issue of a trusted identification system for the Internet. This is one place that the administration has at least provided a plan to move ahead, but lacking few specific mileposts and timelines. According to White House officials, the National Institute of Standards and Technology (NIST) will work with private companies to spur development and shepherd adoption of trusted ID technologies. The Department of Commerce (DOC) has released its National Strategy for Trusted Identities in Cyberspace (NSTIC) and intends to encourage a wide-ranging market for authentication schemes… perhaps even an interoperable one. What is clear is that the username/password combination is no longer secure enough, and something has to change. How do we know your credentials are real and are being used by you? The NSTIC-described trusted ID technologies would allow online users to use credentials across multiple websites as part of the strategy administration officials “hope” that yet-undefined multiple-trusted ID technologies will emerge… and of course consumer use of the technologies will be voluntary. Left open to question is “voluntary, voluntary,” or only voluntary depending on which sites you wish to visit.

Government's Role in Monitoring and Defense

We recently conducted a survey that asked whether the public would approve of DoD participation in protecting the .gov and .com domains. The majority of our respondents seemed to think the public wouldn't be too bothered by such a role by the military. Jim Harper of the libertarian Cato Institute, commenting on "Perfect Citizen," a program employing NSA to detect cyber assaults on private companies and government agencies running critical U.S. infrastructure, is certainly in favor of an informed public. In an opinion piece he wrote last year, Harper argues that the national security apparatus overstates the threat of a "Cyberwar" while cloaking many programs in secrecy. He believes we need a healthy, public debate about the government's role in protecting privately owned resources:

> *"If there is to be a federal government role in securing the Internet from cyberattacks, there is no good reason why its main components should not be publicly known and openly debated. Small parts, like threat signatures and such--the unique characteristics of new attacks--might be appropriately kept secret, but no favor is done to any potential attackers by revealing that there is a system for detecting their activities.*
>
> *A cybersecurity effort that is not tested by public oversight will be weaker than ones that are scrutinized by private-sector experts, academics, security vendors, and watchdog groups.*
>
> *Benign intentions do not control future results, and governmental surveillance of the Internet for*

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

"cybersecurity" purposes may warp over time to surveillance for ideological and political purposes."[11]

In terms of cybersecurity accomplishments, Congress seems to be no more effective than the administration. As mentioned earlier, there have been multiple pieces of proposed legislation aimed at regulating or securing the Internet, but most have failed in gaining passage. Further, committee fiefdoms abound, and as a result, many of the proposed regulations run counter to other contemplated laws. An example of this is the "Cybersecurity and Internet Freedom Act" now before Congress. First introduced as the "Protecting Cyberspace as a National Asset Act" by Senators Lieberman, Collins, and Carper in June 2010, it received a makeover and renaming in February 2011. In spite of this, there remains much disagreement on what the bill actually authorizes the government to do when responding to cyber-related emergency situations. The ambiguous language of this legislation has prompted criticism from both sides of the aisle, causing Senator Lieberman to spend more time trying to dispel the notion that the bill doesn't actually contain an Internet "kill switch" provision than he spends on advocating for its passage.

Regulation and Liability

Is Congress's lack of action in cybersecurity a good or bad thing? Will our security be enhanced by more government regulation or a market-oriented approach that includes, among other things, tort liability? In a 2005 paper, Wayne Crews of the Competitive Enterprise Institute had this to say:

"We face unprecedented information security vulnerabilities in our hyper-networked, global economy. Leaving the path clear for private, technical, market, and contractual solutions, and avoiding governmental mandates that impede contractual liability and insurance markets, should take priority. Embracing legislation or mandates can mean locking in collective "solutions" that may be hard to correct, undermining information security rather than enhancing it. Policymakers, along with the computing and infrastructure industries, should think carefully before implementing further federal regulation over risk allocation.

The principle for cyber-risk allocation, as much as one can be defined, is that government's protection function should not overburden the ability of markets to self-insure or self-protect via technology, contractual liability and insurance instruments. Although there is not always a bright line, government must better distinguish between proper public and private responsibilities in information security, and avoid dictates that interfere with these private alternatives as technologies or other conditions change. Interventionist approaches will create jealousies among players, and lead to a politically driven hodgepodge of liabilities and immunities.

Uncritical government assumption of responsibility for network and critical infrastructure risks can roll back progress without contributing to information security, cybersecurity or even national security." [12]

In advocating for a liability-based approach during the Hathaway Commission's 60-Day Review in 2009, Cato's Harper offered this perspective:

"A liability regime is better at discovering and solving problems than regulation. Owners faced with paying for harms they cause will use the latest knowledge and their intimacy with their businesses to protect the public. Like regulation, a liability regime won't catch a new threat the

[11] "Perfect Citizen": Congress' Perfect Failure, by Jim Harper, 8 July 2010, available at http://techliberation.com/2010/07/08/perfect-citizen-congressperfectfailure/

[12] "Cybersecurity Finger-Pointing: Regulation vs. Markets for Software Liability, Information Security, and Insurance" by Clyde Wayne Crews, Competitive Enterprise Institute, 31 May 2005; available at http://cei.org/pdf/4569.pdf

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

first time it appears, but as soon as a threat is known, all actors must improve their practices to meet it. Unlike regulations, which can take decades to update, liability updates automatically.

Liability also leaves more room for innovation. Anything that causes harm is forbidden, but anything that does not cause harm is allowed. Entrepreneurs who are free to experiment will discover consumer-beneficial products and services that improve health, welfare, life, and longevity.

Liability rules aren't always crystal clear, of course, but when cases of harm are alleged in tort law, the parties meet in a courtroom before a judge, and the judge neutrally adjudicates what harm was done and who is responsible. When an agency enforces its own regulation, it's not neutral: Agencies work to "send messages," to protect their powers and budgets, and to foster future careers for their staffs.

Especially in the high-tech world, it's hard to prove causation. The forensic skill to determine who was responsible for an information age harm is still too rare. But regulation is equally subject to evasion. And liability acts not through lawsuits won, but by creating a protective incentive structure.

One risk unique to liability is that advocates will push to do more with it than compensate actual harms. Some would treat the creation of risk as a "harm," arguing, for example, that companies should pay someone or do something about potential identity fraud just because a data breach created the risk of it. They often should, but blanket regulations like that actually promote too much information security, lowering consumer welfare as people are protected against things that don't actually harm them.

As complex and changing as cyber security is, the federal government has no capability to institute a protective program for the entire country. While it secures its own networks, the federal government should encourage the adoption of state common law duties that require network operators, data owners, and computer users to secure their own infrastructure and assets. (They in turn will divide up responsibility efficiently by contract.) This is the best route to discovering and patching security flaws in all the implements of our information economy and society."[13]

Although we share the enthusiasm for minimalist government expressed by both Messrs. Crews and Harper, we also wonder whether private firms operating under a liability-based cybersecurity regime will be entirely forthcoming in sharing vulnerabilities and other details with the government and public prior to and/or following a cyber attack.

International Norms of Behavior

Finally, there's the issue of international norms of behavior. According to a report by Voice of America, the U.S. joined last year with 14 other nations in signing a United Nations agreement to work together to develop "...international standards for conduct over the Internet, sharing information about each country's cybersecurity laws, and helping less-developed nations strengthen their computer defenses."[14] While we believe some good can come out of such efforts, we have reservations about blindly pitching in with the United Nations, thus losing our autonomy and shredding our Constitution. One concern in particular has to do with the U.N.'s emphasis on preventing so-called "hate speech."

[13] "Government-Run Cybersecurity? No, Thanks" by Jim Harper, Cato Institute, 13 March 2009, available at http://www.cato.org/pub_display.php?pub_id=11450

[14] "15 Countries Outline Principles on Cyber Security," *VOA News*, 17 July 2010, available at http://www.voanews.com/english/news/science-technology/15-Countries-Outline-Principles-on-Cyber-Security-98661289.html

Gen (Ret) Ron Keys, RK Solution Enterprises
Larry K. McKee, Jr., NSCI
May 6, 2011

Addressing an "Unlearning Intolerance" seminar on the danger of "cyberhate" in 2009, U.N. Secretary-General Ban Ki-moon said, "There are those who use information technology to reinforce stereotypes, to spread misinformation and propagate hate."[15] The U.N. chief has since pressed for actions that would limit speech on the Internet. So again, the security issue is being sidetracked by another niche issue, and the technical/policy problem of securing the medium is being thwarted with the policy/moral issues of what travels over the medium.

This latest agreement to work with the U.N. joins a growing list of similar initiatives that have resulted in very few actual decisions being made. Perhaps we will soon reach some consensus in establishing international norms in such areas as cyber crime, cyber "warfare," and armed response to cyber attacks, among others. As mentioned earlier, the recent U.S.- Russia Critical Terminology Foundations agreement may be an important first step.

Conclusion

It is our belief that the administration has stalled in its efforts to secure the Internet. However, it is certainly not too late to empower the appropriate people and organizations with the necessary authorities to improve the situation rather dramatically in a short amount of time. We certainly have the technical know-how; what is left is to identify and implement focused strategy and policies and define clear roles and responsibilities that will enable us to use that know-how to protect individual freedoms while providing a more safe, secure, and reliable cyberspace domain for government, industry, academia, and the average United States citizen. Most critically, who's in charge, what's important, and then concrete steps to harden the net, secure critical infrastructure, share "share-able" information, and internationalize cooperation. We believe the recommendations above can significantly aid in accomplishing these objectives.

[15] "UN urges fight against hate speech in cyberspace," AFP News Agency, 17 June 2009, available at http://www.un.int/wcm/webdav/site/ui/shared/documents/Google_News.pdf

"Maryland High School Gets Cyber Curriculum," The New New Internet, Feb. 15, 2011, available at http://www.thenewnewinternet.com/2011/02/15/maryland-high-school-gets-cyber-curriculum/

> Maryland's Meade High School will be the first in Anne Arundel County to have cybersecurity curriculum intertwined into existing computer classes. The modern curriculum will hopefully lead more students to study and enter into the crucial and growing cybersecurity professional job market. Coordinators hope the new mix will be extended into other area schools.

"New UMD Cyber Center to Strengthen Public-Private Partnerships," The New New Internet, Oct. 21, 2010, available at http://www.thenewnewinternet.com/2010/10/21/new-umd-cyber-center-to-strengthen-public-private-partnerships/

> The University of Maryland will open a new cyber center in an effort to train more students and professionals in the growing field of cybersecurity. The Maryland Cybersecurity Center will also work with businesses to implement technologies researched and studied at the Center.

"Booz Allen, UMUC Partner to Offer Cybersecurity Degrees," The New New Internet, Oct. 20, 2010, available at http://www.thenewnewinternet.com/2010/10/20/booz-allen-umuc-partner-to-offer-cybersecurity-degrees/

> University of Maryland University College began offering three graduate certifications to Booz Allan Hamilton employees in fall 2010. The certifications, available online through UMUC, will be available to the general public in spring 2011. The certifications focus on either foundations of cybersecurity, cybersecurity policy or cybersecurity technology, and credits are applicable to UMUC's full Master's of Science in Cybersecurity or Cybersecurity Policy degree.

"Northrop Grumman Promotes Safer Web Practices by Launching Cyber Academy," Cooper Smith, The New New Internet, Oct. 6, 2010, available at http://www.thenewnewinternet.com/2010/10/06/northrop-grumman-promotes-safer-web-practices-by-launching-cyber-academy/

> To commemorate National Cybersecurity Awareness Month, Northrop Grumman announced several initiatives to bring cybersecurity into the spotlight. The corporation held an educational workshop "designed to inspire and excite local high schoolers to pursue a career in cybersecurity." NGC also launched a new training facility for cybersecurity professionals and began more research projects.

"HP-backed IT degree aims to deliver industry-ready graduates," Jenny Williams, Computer Weekly, Oct. 6, 2010, available at http://www.computerweekly.com/Articles/2010/10/06/243194/HP-backed-IT-degree-aims-to-deliver-industry-ready-graduates.htm

> HP will help provide practical work experience to 30 computing students at the University of the West of England in 2011. The selected students will be given internships at HP or with HP partners. The collaboration between HP and UWE hopes to "increase graduates' level of work experience and employability."

"SAIC Opens Cyber Center in Maryland," Jack Moore, The New New Internet, Sept. 27, 2010, available at http://www.thenewnewinternet.com/2010/09/27/saic-opens-cyber-center-in-maryland/

> SAIC opened its new center in Columbia, Md., for developing and delivering innovative cybersecurity solutions. The Cyber Innovative Center has a lab for technical solutions, research and development, training and support spaces, and demonstration, prototyping and proposal

solution support areas. The center will continue Maryland's foothold as one of the epicenters for cybersecurity education and innovations.

"Northrop Grumman Partners with U of Cincinnati for Cyber Education," Michael Cheek, The New New Internet, Aug. 10, 2010, available at http://www.thenewnewinternet.com/2010/08/10/northrop-grumman-partners-with-u-of-cincinnati-for-cyber-education/

The University of Cincinnati and Northrop Grumman Corporation will work together to provide Northrop Grumman employees and others a master's degree in computer science with a focus on cyber informatics. The classes will be taught both on campus and at the NGC Xetron facility in Cincinnati.

"NYU-Poly Launches New Cyber Grad Program," Michael Cheek, The New New Internet, July 29, 2010, available at http://www.thenewnewinternet.com/2010/07/29/nyu-poly-launches-new-cyber-grad-program/

The National Science Foundation provided a $2.85 million grant that will fund a new graduate program through the Polytechnic Institute of New York University. The INSPIRE (Information Security and Privacy): An Interdisciplinary Research and Education Program for engineers and scientists will address IT security and privacy issues as well as "an understanding of the interplay between security, public policy, law, psychology and economics."

"New cybersecurity degree program designed to fill workforce needs," Byron Acohido, USA Today, July 19, 2010, available at http://content.usatoday.com/communities/technologylive/post/2010/07/new-cybersecurity-college-program-designed-to-fill-workforce-needs-

The University of Maryland University College has seen more than 200 applicants for its new online degree programs aimed to enhance cybersecurity knowledge. The cybersecurity profession is in critical need for a larger workforce, and individuals in UMUC's new degree programs will study a curriculum that "has a direct tie to the collaborative work done by the Center for Strategic and International Studies' Commission on Cybersecurity for President Obama."

"SAIC Forges Cyber Education Partnership with Capella University," Michael Cheek, The New New Internet, July 12, 2010, available at http://www.thenewnewinternet.com/2010/07/12/saic-forges-cyber-education-partnership-with-capella-university/

To enhance its cybersecurity research and solutions, SAIC is partnering with Capella University to create an educational program for its employees. The program will be for those employees who pursue Capella's master's degree in Information Assurance and Security.

"New York Puts Up $2.78 Million for Cyber Training," Michael Cheek, The New New Internet, July 6, 2010, available at http://www.thenewnewinternet.com/2010/07/06/new-york-puts-up-2-78-million-for-cyber-training/

A $2.78 million state grant will help give cybersecurity skills to New York residents. The grant will fund a training program through the Mohawk Valley Community College. Sen. Chuck Schumer said the program will help train New Yorkers for "a generation of high-tech jobs."

"Harris Opens Cyber Integration Center," Michael Cheek, The New New Internet, May 21, 2010, available at http://www.thenewnewinternet.com/2010/05/21/harris-opens-cyber-integration-center/

> Harris Corporation will create the U.S.'s first cyber integration center, which will be located 120 nautical miles from "what we believe the center of cyber activity in the United States is right now." Its location will allow for abundant use by federal businesses along with private commercial industries. Harris will also aquire SignaCert, Inc.

"SAIC Partners with NYU-Poly to Provide Education to Workforce," Michael Cheek, The New New Internet, May 5, 2010, available at http://www.thenewnewinternet.com/2010/05/05/saic-partners-with-nyu-poly-to-provide-education-to-workforce/

> SAIC and the Polytechnic Institute of New York University will work together to provide top-performing SAIC employees with master's degrees in cybersecurity. The degree will be earned with a combination of in-class and online instruction. Lab assignment will be performed through the school's Virtual Security Lab, a.k.a. VITAL, which is the U.S.'s only university-based virtual cybersecurity lab.

"SAIC Donates $250,000 to the U.S. Naval Academy Foundation to Support the Creation of a Center for Cyber Security Studies," PRNewswire, April 8, 2010, available at http://www.prnewswire.com/news-releases/saic-donates-250000-to-the-us-naval-academy-foundation-to-support-the-creation-of-a-center-for-cyber-security-studies-90204397.html

> The U.S. Naval Academy Foundation received a $250,000 donation from the Science Applications International Corporation. The donation will go toward the creation of the Center for Cyber Security Studies, which will provide cybersecurity and cyberwarfare education for midshipmen. The Navy's 10th fleet will serve as a component to the U.S. Cyber Command.

"UAE Offers Cybersecurity Degrees," Michael Cheek, The New New Internet, March 8, 2010, available at http://www.thenewnewinternet.com/2010/05/05/saic-partners-with-nyu-poly-to-provide-education-to-workforce/

> The United Arabs Emirates has joined the wave of cybersecurity education. Its Zayed University has begun offering a Masters of Science in Information Technology with a concentration in Cyber Security Digital Forensics. The first fifteen to graduate with the degree were all members of the Abu Dhabi Police and will work to combat cybercrime in the UAE.

"Lockheed Martin Invests In Cyber Security Talent and Workforce Development," Darkreading, Jan. 20, 2010, available at http://www.darkreading.com/security/news/222301688/lockheed-martin-invests-in-cyber-security-talent-and-workforce-development.html

> To fulfill the need for a knowledgeable cybersecurity workforce, Lockheed Martin has invested more than $1 million in recruiting, scholarships and training in the cybersecurity field. Lockheed Martin has also implemented a Cyber University to better prepare and provide certification for individuals in the cybersecurity profession.

"Earn a free masters degree in the Federal Cyber Corps," Cybersecurity Update, Federal News Radio, Nov. 12, 2009, available at http://www.federalnewsradio.com/?nid=15&sid=1810451

> The Scholarship for Service program added the Monarch Scholarship to its bounty. Recipients can receive a Master's degree in the cybersecurity field, in addition to money, in exchange for

working two years at different government agencies upon graduation. Also, the FBI is behind on its Sentinel electronic information and case management system.

"Cyber Consortium Gets $2.7 Million Grant," Tim Talley, Enterprise Security Today, Oct. 16, 2009, available at http://www.enterprise-security-today.com/story.xhtml?story_id=69519

The Cyber Security Education Consortium received a three-year, $2.7 million grant from the National Science Foundation to aid the 32 institutions that make up the consortium. The grant will fund programs for cyber education security and work force development training to help combatant the out-sourcing of high-tech jobs.

"Federal Funding for AASU Cyber Security Initiative," WSAV TV, NBC affiliate, Feb. 26, 2009, available at http://www2.wsav.com/news/2009/feb/26/federal_funding_for_aasu_cyber_security_initiative-ar-135204/

Armstrong Atlantic State University's Cyber Security Research Institute will begin offering a graduate degree in cyber affairs and security with the help of federal funding. Rather than just offering a graduate certificate, funding secured by Congressman Jack Kingston will allow the program to grow. Several federal law enforcement agencies, along with students, utilize the Institute to receive cyber threat and security education.

"Carnegie Mellon University – CyLab," CMU, available at http://www.cylab.cmu.edu/

Carnegie Mellon University's CyLab is purposed to research and educate both students and the broader community about cybersecurity. The CyLab reaches out to public and private institutions to further develop Information Assurance professionals.

"Cyberethics for Teachers," Department of Justice, available at http://www.justice.gov/criminal/cybercrime/rules/lessonplan1.htm

"Cybercrime.gov," Department of Justice, available at http://www.justice.gov/criminal/cybercrime/cyberethics.htm

The Department of Justice has numerous tools for helping teachers to develop teaching plans aimed at educating students about cyberspace, cyberethics and cybersecurity.

"iKeepSafe Kids," Internet Keep Safe Coalition, available at http://ikeepsafe.org/iksc_kids/

A partnership of governors, and/or first spouses, attorneys general, public health and educational professionals, law enforcement and industry leaders have developed a website aimed at teaching and keeping children safe while using the Internet. There are tools available for parents, educators, policymakers and children. The link is to the mascot Faux Paw's Fun Zone, which has different links to make learning about cybersecurity for kids fun.

"Lessons by Grade Level," Common Sense Media, available at http://cybersmartcurriculum.org/lessonsbygrade/

Common Sense Media has taken over CyberSmart! Curriculum, which provides teaching lessons on cybersecurity for grades kindergarten through twelfth. Lessons can be integrated into already existing plans.

"NetSmartz for Educators," National Center for Missing and Exploited Children, available at http://www.netsmartz.org/Educators

NetSmartz provides information, teaching materials and presentations on Internet safety to educators at all levels.

"Online safety & civility," SafeKids.com, available at http://www.safekids.com/

SafeKids.com offers tips and solutions to some of the latest Internet uses aimed at and used by children, such as advice on the latest PlayStation data breach, safety with Facebook, online predators and charity scams.

"Pennsylvania Cyber Security," Pennsylvania Information Security Office, available at http://www.portal.state.pa.us/portal/server.pt?open=512&objID=496&&mode=2

Pennsylvania's Information Security Office has created Dewie the Turtle to be the mascot for Internet safety. Kids are invited to learn how safe they are when surfing the web and are given tools to enhance their web security.

"Stay Safe Online," National Cyber Security Alliance, available at http://www.staysafeonline.org/

The National Cyber Security Alliance has centralized its focus on keeping individuals safe online by providing information to parents, primary and secondary educators, and businesses on how to best protect and teach people, with an emphasis on children, about cybersecurity. There are links to lesson plans for k-12 teachers along with studies on the state of cyber education. The NCSA and Microsoft compiled their own list of cybersecurity resources available to teachers and parents, which can be found at http://www.staysafeonline.org/sites/default/files/resource_documents/k12%20additional%20resources%20final%20(2).pdf

"Technology: Cyber Security," USA Today, available at http://www.usatodayeducate.com/wordpress/index.php/technology-cyber-security

USA Today, in partnership with the National Cyber Security Alliance and the U.S. Department of Homeland Security, has provided lessons and links for teachers wanting to integrate cyber ethics and security into their curriculum.

"WiredSafety: the world's largest Internet safety, help and education resource," WiredSafety, available at http://www.wiredsafety.org/

WiredSafety has provided information on cyber threats and safety issues that most everyone faces, but with an emphasis on children.