

MPF Report

Cyber Security Conference

Forum Participants

Moderated by Paul B. Kurtz and Michael A. Sheehan. MPF Fellows Karen Greenberg and R.P. Eddy also moderated panels. Key participants included:

Richard A. Clarke
R. Rand Beers
Kenneth Minihan
Scott Borg
Dave Cullinane
Jerry Dixon
Rhonda MacLean
Eugene Spafford
Paul Twomey

About the Madison Policy Forum

Founder & President:

Vincent Viola

Executive Director:

Michael A. Sheehan

Fellows:

Karen Greenberg

R.P. Eddy

Robert Windrem

The Madison Policy Forum was created to advance rigorous, nonpartisan policy review of key national security issues. In the tradition of our fourth President, James Madison, our goal is to promote informed public discussion, which he considered a critical component of an effective democracy.

<http://madisonpolicyforum.org>



Richard A. Clarke delivering keynote address at MPF Cyber Security Conference

The Madison Policy Forum convened a high-level meeting of cyber security experts to assess the cyber threat to the United States. The Forum, held on October 27, 2009 at the Waldorf-Astoria in New York, approached the cyber threat from a skeptical point of view, questioning whether the current level of concern is warranted given the known facts about the threat.

Based on the findings from the discussion, though most Americans do not yet feel the sting of internet-based attacks, the threat is real and growing. The cyber threat deserves more attention, as both a criminal problem and as a form of unconventional warfare. The Forum outlined some key steps that should be considered to improve our nation's readiness for this growing threat.

Cyber Crime: Threats and Trends

The last three years have seen tremendous growth in both the number and sophistication of cyber criminal acts. Cyber criminals are targeting large financial institutions as well as end-users in order to gain information to generate criminal profits.

Key Findings

- **Cyber crime is big business.** Some estimates rank cyber crime above the international drug trade in terms of revenue generated. Home computers are being targeted to collect credit card account information that can be used to stamp blank cards and make fraudulent purchases.

Purchased goods are then resold for cash on black markets. Other schemes include using botnets (software robots) to conduct distributed denial of service (DDoS) attacks and then extorting cash from the victims in order to turn off the attack.

- **Cyber criminals exploit poor international law enforcement coordination.** Cyber criminals take advantage of national boundaries and weak enforcement regimes to reduce the risk that they will be caught. The jurisdictional boundaries that most cyber attacks cross make prosecution difficult. Cyber crime remains a very low risk and high reward enterprise. Without fear of prosecution there is little if any deterrent to cyber crime. There is a definite need for treaties to extend the reach of U.S. law enforcement and to criminalize these acts abroad and for western governments to provide law enforcement assistance. A consortium of IT businesses has spent millions helping developing countries write laws and train law enforcement. The approach has been fairly successful, but the number of countries these efforts include is small.
- **Malware is evolving faster than countermeasures.** By some estimates, a new piece of malware (malicious software) is created every 2.2 seconds. Microsoft sees one million new pieces of malware each day. Criminal gangs may be outspending the government and IT security firms on research and development. Many of these newly created pieces of malware are developed to target specific vulnerabilities on individual sites, revealing an extraordinary level of sophistication on the part of today's cyber criminals. Criminal gangs have also begun to penetrate the supply chain, contaminating hardware as well as software.
- **Prosecutors need better incentives to go after cyber crime.** There have been only sixty-two successful prosecutions of cyber crime in the United States since 1998. US attorneys are not interested in pursuing cases because of the low rate of success and because the sums in question are insufficient to warrant a full investigation. The federal government should consider creating incentives for the prosecution of cyber crime by U.S. attorneys or should create a separate, dedicated unit to do it.
- **The business case for security should be strengthened.** The cost of conducting transactions on the web is a fraction of the cost of conducting transactions through a brick and mortar operation. If customers do not believe that their online transactions are secure, however, they may stop using web-based systems and return to the teller windows and storefronts. Businesses should be encouraged to measure these costs and adjust customer preferences over time. The adoption of advanced security controls on banking websites leads more users to enroll in online banking, which reduces overall operating costs. The story of how these initiatives contributes to the bottom line needs to be told more often and more clearly.

“No single action has done more to improve security in the financial sector than California’s breach notification laws. Congress needs to adopt reasonable incentivizing legislation to promote better security.”

Rhonda McClean, former CIO Barclay’s

Cyber Warfare

While cyber crime and malware affect system performance, these problems do not threaten system survival. The U.S. national security interest is threatened by a structured, state-level effort that is planned, methodical, and exercised by professional entities. The nations behind these offensive cyber preparations are serviced by robust intelligence and have clear target lists. The actual “hackers” may be directly in the employ of military or intelligence units or they may be private criminal organizations with national affiliations. This refined and structured threat could cause harm that would be tantamount to an act of war. China and Russia represent the biggest challenge with regards to illegal cyber activity that is either directly supported, condoned or ignored by their respective governments.

Key Findings

- **Cyber warfare should be understood in the context of military history.** Since the era of siege warfare, competing nations have recognized that the source of an enemy's strength was not its army but the economic power that allowed that army to be raised and sustained. Siege warfare was the advent of purposeful economic warfare. In the twentieth century, Billy Mitchell and other early proponents of strategic bombing realized that airplanes could be used to skip over the battlefield to attack the economy. Now, without the use of bombs, countries can achieve that objective.



LTG (USAF Ret.) Kenneth A. Minihan discussing cyber warfare

- **The line between espionage and acts of war is eroding on the web.** In the twentieth century, countries recognized a distinction between intelligence activities and acts of war. That distinction may not hold in the information age. The danger today is that warfare activities are being conducted under the guise of espionage. Cyberspace should be thought of as a domain in which low intensity conflict is always occurring. We are always in a state of either crisis or war in cyberspace; there are no pauses in conflict for peace or peacetime preparation for crisis or war. That is very destabilizing.
- **Intellectual property theft may be a form of cyber economic war.** At a strategic level, the US military is beginning to view the loss of intellectual property not as an economic security issue, but as a national security issue. The scale of loss has not yet been quantified, nor has the impact on our national security and economic competitiveness.
- **There is a nexus between “cyber war” and cyber crime.** There is evidence of Russian criminal cooperation in a number of attacks including those on Estonia in 2007 and Georgia in 2008. In both cases, it is more likely that the criminal elements were quietly encouraged to carry out the attacks rather than paid to carry them out. The Chinese government is also thought to rely heavily upon private hacking groups. If cyber crime were reduced by the elimination of vulnerabilities that cyber criminals exploit, it would also raise the bar for state-level actors.
- **“Traditional” cyber terrorism does not yet exist.** Most terrorists continue to use the Internet for training, communicating, fund-raising and distributing propaganda. The infrastructure the jihadi community has built for these purposes is extremely sophisticated. Cyber attacks by terrorist organizations have been limited to the defacement of Israeli websites and DDoS attacks also against Israel. Terrorist organizations may have a more difficult time acquiring criminal capabilities because the terrorist groups cannot provide protection or a safe-base of operations and because engaging in terrorist activity could threaten the survival of their criminal enterprises. Moreover, states that are more lenient with cyber criminals often have their own concerns with jihadist groups. Russia and China, for example, would not tolerate any cooperation with such groups.
- **The electric grid may be vulnerable to attack and merits further study.** Concern is mounting that cyber attacks could target the electric power grid with devastating consequences. Monitoring cyber attacks reveals a significant degree of scanning of ports that are used for the computer control systems that manage the grid. These ports have other uses but the scanning could indicate a high level of interest in finding and identifying

“Our adversaries don’t have the same vulnerabilities in cyber warfare, so at some point their action may provoke an asymmetrical/kinetic response from us.”

Lieutenant General Kenneth A. Minihan, former NSA Director

pathways into these critical networks. IT security auditing firms are routinely able to penetrate power companies' administrative networks and from there gain access to control systems. Wireless communication systems used for grid computer systems networks can also be hacked. Many power companies have begun to use Voice over Internet Protocols (VoIP) even in control rooms. These systems are very vulnerable and can be used to gain access to other systems on the same network. In the spring of 2009 the *Wall Street Journal* reported that foreign agents had penetrated the power grid and had laced it with logic bombs and backdoors. Earlier in the year, the *Washington Post* reported that a country in South America had their power grid taken over by criminal gangs that made ransom demands.

Current U.S. Policy

Upon taking office, the Obama Administration announced plans to conduct a 60-day policy review of cyber security. While conducting the review, the Obama Administration directed that all ongoing activities under the Critical National Cyber Initiative (CNCI) continue throughout the initial 60-day review. Following completion of that review, those efforts were continued. The new administration has pushed forward on developing a National Cyber Incident Response Plan and is working to complete the implementation of the Einstein II intrusion detection system and to move forward on the Einstein III intrusion prevention system. The Department has also consolidated all cyber-related offices under the Deputy Under Secretary of the National Programs and Preparedness Division and combined several entities into the National Cybersecurity Communications and Integration Center. In December of 2009, President Obama appointed Howard A. Schmidt as White House Cybersecurity Coordinator. Schmidt is a well-respected leader against the cyber threat, competent in the arcane ways of Washington, and is well equipped to help lead on this pressing issue. Despite these activities, the Forum found that the United States lacks a clear national strategy for confronting the threats we face in cyberspace.

Key Findings

- **Threat-briefings should be used to promote additional private investment.** The most basic step the US government should take is to increase information sharing with the private sector, particularly on threats. When a handful of financial industry executives received a one-day briefing from the intelligence community in the fall of 2008, they reacted by increasing investments and prioritizing security improvements. One simple way to increase information sharing would be to eliminate the fees for membership in ISACs by qualified companies.
- **A high priority must be placed on training a sufficient number of personnel.** Many organizations have security devices and infrastructure but do not have the personnel to monitor them or to respond to incidents when detected. In cyberspace, the real weapons are not worms or viruses, but the people who design and build them and the people who can defend against them. The United States may not be producing enough security professionals to compete with countries that are producing them at much higher rates.
- **The United States needs a clear agenda for international engagement on cyber security.** Aspects of the US agenda should include: 1) Commitment to an international approach to cyber security that includes specific action items; 2) Promotion of secure technical standards for Internet communications through the Internet Engineering Task Force; 3) Engagement with friendly elements within foreign governments on common security concerns; and 4) Development of an international response framework to assist countries when they come under cyber attack.

“Stealing intellectual property via cyber crime makes research and development free for competing countries’ industries, which means that they have a lower cost structure, with an advanced product set. Effectively, our loss of intellectual property via cyber crime is taking away our strategic/comparative advantage—research and development—in the global marketplace.”

Richard A. Clarke, former White House Cyber Czar

- **The Obama Administration has continued the Bush Administration's voluntary approach.** The President has stated that he prefers a partnership approach with the private sector to secure critical infrastructure. The Department is focusing on information sharing and capacity building and may consider standard setting within specific critical sectors. DHS has the authority to set standards under law, though the adoption of these standards is voluntary. Congress should consider adopting reasonable incentivizing legislation that would promote security. Privacy breach notification laws have had a tremendously positive effect on security.

Research Agenda

The Madison Policy Forum is pursuing the following projects on cyber security:

- **Cyber Defense and Security, The State of the Field.** The policy community is in the early stages of addressing cyber defense and cyber security. Given the urgent need to move the ball forward on this issue, it may be in the interest of the policy community to convene a "meta-conference" of all the institutions that have launched cyber security initiatives to identify gaps and overlap and lay out a consensus research and policy development agenda.
- **Securing the Smart Grid.** The Obama Administration has invested \$3.4 billion in "smart grid" technologies that use the Internet to manage the power system and improve efficiency, but cyber security experts worry that the rush to implement these technologies could increase the grid's vulnerability to cyber attack. Many believe that the grid is already over-reliant on Internet-based technologies and is vulnerable to cyber attacks that could have devastating consequences. This project seeks to separate fact from fiction on the threats to the power grid and lay out a strategy for how investments to make the grid "smart" can also make it safer, stronger and more reliable.



Michael A. Sheehan (front) with Paul B. Kurtz leading the discussion at the conference



Founder and President of the Madison Policy Forum Vincent Viola with Richard A. Clarke