Defending Cyberspace:

The View from Washington

Howard Schmidt
Cybersecurity Coordinator
The White House

An Interview with Cameron Parsons and Mustafa Safdar
Providence, RI, 11 April 2011

Howard Schmidt is the cybersecurity coordinator at the White House. He previously served as president of the Information Security Forum and the Information Systems Security Association. He has also held various positions in the private sector, including chief security officer at Microsoft.

Brown Journal of World Affairs: Can you describe the state of cybersecurity policy in the United States and the nature of the cyberthreat?

Howard Schmidt: That's probably the broadest question I think anyone could ask. It goes from one end of the spectrum to the other, from protecting users to building trust in day-to-day transactions like e-commerce to issues of cyberespionage. We are also looking at creating an environment where we have the ability to better defend cyberspace, including the dot-mil environment.

From the U.S. perspective, we are better off in a lot of these areas than we were a year ago, but there is no shortage of forces trying to undermine some of the efforts that we put forth. We need to continue to work not only to recover from some of the latest dilemmas that we have been dealing with, but also to anticipate activity in new areas and build security and privacy controls into the future technology we roll out.

Journal: In an interview you gave to *Wired* magazine in June, you said "there is no cyberwar and that it is a terrible metaphor." Can you elaborate on why the term "cyberwar" is problematic?

Schmidt: When you are in some sort of conflict, one of the goals is always to affect the communications of your adversary. In the early days of the West, that meant climbing up the telephone pole and snipping the telegraph wires so the enemy couldn't communicate. But since then, communication systems have expanded to different channels—they are no longer just single wires, a phone call, or a radio transmission. Cyberspace has become one of these critical communication systems. When you look at conflicts, since cyberspace is a communication channel, it would be a target for disruption. One reason for the concern in this area is that cyberspace is relied upon for much more than just military communication. The vast majority of communication is for civilian and economic applications.

The other piece of this involves the overuse of the phrase "cyberwar." Anytime someone commits a denial-of-service attack or someone intrudes into a system to steal intellectual property, it's not a cyberwar. This kind of hype is beneficial to no one. We, as a society—not just the government, but citizens, businesses, entertainers, and journalists—depend on that cyberinfrastructure to be there. The idea of creating this environment where we have "mutually assured disruption" is not an environment that anybody would favor.

Journal: Do you believe the threat has been exaggerated?

Schmidt: I do not know if I would call the threat "exaggerated," "enflamed," or anything else. I think people like to use words and terms relevant to warfare and terrorism. Those are words that get people thinking, and sometimes people use those terms without really thinking about the larger implications of their use. We have seen this throughout history; it always seems easier to frame issues as a "war," such as a "war" against people driving without seatbelts or a "war" against drugs. We have to be very precise because words do matter—particularly when you are looking at international relationships. We all depend on the Internet; we all depend on the communications systems. We have to be very precise in our terminology. We see identity theft and credit card fraud; we see theft of intellectual property; we see disruption through denial-of-service attacks or malicious activities; we see the creation of malware for personal advantage. Going forward, we have to first put these problems in the proper context as we look for solutions.

Journal: Now, we mentioned coordination briefly. One of the chief criticisms of federal cybersecurity policy has been poor interagency coordination and a lack

of collaboration. What has your office done to improve the situation?

Schmidt: I think there are a couple of steps that we've taken. One is the document we are now shoring up: the National Cyber Instant Response Plan (NCIRP), which the Department of Homeland Security is coordinating. That document was built and informed by a series of what we call "cyberstorm exercises." The most recent one was last fall (Cyber Storm 3), in which we looked at the whole government inclusive of our private sector and international partners. We walked through how to coordinate response actions to an event that has the ability to escalate into a national- or international-level event. By conducting these exercises and drafting the NCIRP, we are trying to identify what players we are missing, what legal problems might arise, and what communication paths we need to establish beforehand. We are not sure how an event like this would unfold, but we want to be as best prepared as possible. NCIRP really gives us the ability to pool resources of the government and the private sector as well as international partners who are key stakeholders.

Journal: Could you elaborate on the private sector's role in protecting critical infrastructure?

Schmidt: Back in 1998, President Clinton created a Presidential Decision Directive (PDD) known as PDD63 to acknowledge and then answer the following dilemma: Computers run our everyday lives; computers are integrated into everything we do; we have tremendous dependency on them. What's the role of government? What's the role of the private sector?

PDD63 called for the private sector to voluntarily organize among itself because the vast majority of owners and operators of critical infrastructure—the power generating. transportation, information technology, and water systems—were, and are, in the hands of the private sector. If you think back to the mid-to-late 1990s, it did not get more competitive in the technology world. Asking companies to self-organize and work together was a big step. Second, the PDD63 also noted that critical infrastructure operators did not have any direct relationship with the government. In response, we created sector-specific coordinating councils. For example, the Department of Treasury works with the financial services industry to make sure that the government is sharing information with the private sector and the private sector is sharing information with the government. This started the wave of Information Sharing Analysis Centers (ISAC) that we use today. The first one in 1999 was created in financial services,

where a lot of the financial service industry got together and shared information in three areas: threats, vulnerabilities, and best practices. That way, if there was a particular threat against one financial institution, they would share that information with the rest. Once again, it is the idea that we all swim if everyone is doing the right thing.

With the creation of the Department of Homeland Security, which was given the authority to work with the private sector to identify critical infrastructure, the public-private partnership has grown stronger. We now have mechanisms in place, like the ISACs, to share information and improve everyone's security.

Journal: With the increased emphasis on cybersecurity over the past two years, there has been a marked expansion in private cybersecurity contractors. Major contracts have gone to a number of firms like Lockheed Martin. What are the advantages of outsourcing cybersecurity to the private sector? Is there a danger of overreliance?

Schmidt: Well, I think anytime you are looking at outsourcing anything, you have to make those business decisions based on the level of expertise and the level of training that people need to have. The complexity of networks and the environment today requires a good deal of expertise. Additionally, the complexity and breadth of cyberthreats facing large organizations, such as a federal department, require significant expertise. Instead of duplicating this expertise over and over, it is sometimes possible to group several organizations together and have a single company assist with managing their cybersecurity. These services are called Managed Security Services. This is done in other business aspects, and network security is no different.

Journal: Are we likely to see more of these relationships in the coming years?

Schmidt: I think that we will. One thing we see is that some small pockets of expertise, whether they are former military people or former corporate security experts, form a company and then larger companies looking to add to their security service offerings will acquire them. Again, as with other mergers and consolidations of companies, we will see small- and medium-sized entrepreneurs look for ways to solve security problems, create a good solution, and be acquired. This drives innovation and entrepreneurship in the cybersecurity realm—the same as in other industries.

Journal: Moving toward a more international perspective: the Stuxnet computer worm that targeted Iran's uranium enrichment processors is suspected to be the product of U.S.-Israeli collaboration. What would you say has been the impact of Stuxnet on the cybersecurity community, and does it represent a paradigm shift?

Schmidt: We have recognized for a long time that digital control systems for critical infrastructure were not originally designed to work in an open network environment. I think what we have seen over the past year is the need for a larger focus not only on R&D [Research and Development] and vulnerability management, but also on future design. We need to understand that these threats will exist, and we should build systems that address that fact as opposed to just connecting things to an open network, which makes them increasingly vulnerable. There is certainly increased awareness; it's a technology shift. Discussion of these vulnerabilities has moved from a smaller group of dedicated researchers to a broader audience.

Journal: How do you think international cooperation can benefit cybersecurity? What role, if any, do you think the United States should take in leading a cooperative initiative?

Schmidt: International cooperation has a major role to play in cybersecurity. The Internet is not owned or located in a single country; the challenges we face are not unique. There are two broad categories where we interact internationally. First, there are technical standards that make the Internet work as we know it. There are various international bodies that help make those standards work, whether it is for high-speed wireless connections or Bluetooth. We have an interest in these standards being interoperable, open, reliable, and secure. There are government representatives that participate in all these things. Of course, the United States participates since we not only use but also depend on that technology. We work with our international partners to have a strong seat at the table to make sure that we continue to develop these standards and move technology forward while building those security and privacy controls from the outset.

The Internet is not owned or located in a single country; the challenges we face are not unique.

Second, we have non-technical problems, such as cybercrime, where we must work with other countries on a policy level to address them. Recently, the president released the International Strategy for Cyberspace that laid out how

we, as a whole government, will approach cyberissues.

Journal: People have said that there have been numerous cyberattacks—including a denial-of-service attack against the U.S. government—that have originated from China and Russia. Have these states cooperated with United States and its efforts to investigate the sources of the hacks? Do you believe China, Russia, or other states have supported cybercrime generally and attacks against U.S. systems specifically?

Schmidt: I think in a lot of the cases, countries that have or are developing a dependency on digital systems are struggling with the same problems that we are dealing with. One of the challenges inherent in the way the Internet works has to do with attribution. Just because a system appears to be infected with malware and it seems to be coming from a system of another country does not necessarily mean that a country is particularly sanctioning or is a part of it. We have vulnerabilities in computer systems worldwide, which can be exploited from anywhere in the world, so attribution is very difficult. When we look for bilateral and multilateral international partners, we need to make it clear that we are in this together—not only in government-to-government relationships, but also in government-to-private sector and private sector-to-private sector. We need to make sure that there are no safe havens for cybercriminals from any government. As a government, we look to establish what the norms are in cyberspace, so that we can continue to receive the economic, educational, and cultural benefits of the Internet without worrying about somebody trying to negatively affect these benefits.

We need to make sure that there are no safe havens for cybercriminals.

Journal: Would you say that the Chinese government in particular has been a reliable partner?

Schmidt: The relationship with China is complex and evolving. We engage in dialogue with China on number of issues related to cybersecurity. One of the keys is making sure we both understand topics of concern. We have many areas of discussion and are looking for the best places to make progress on problems affecting everyone.

Journal: On 25 June 2010, a draft of the National Strategy for Trusted Identities in Cyber Space (NSTIC) was released. What progress has been made in

completing the objectives that were set forth in the document?

Schmidt: The National Strategy for Trusted Identities in Cyberspace looks at how we can establish an "Identity Ecosystem" that best preserves anonymity, privacy, and civil liberties, while also creating an environment where we can have greater trust in our online transactions and interactions and feel more comfortable knowing that people are really who they say they are. The Department of Commerce will be hosting the National Program Office (NPO) for the NSTIC and has already begun holding workshops on creating the envisioned "Identity Ecosystem." There are several small efforts that are examples of how the ecosystem could work; the NPO is looking at translating those examples into national level solutions. Also, this is another issue that doesn't just affect us; improving trust in economic transactions is a challenge for the international community.

Journal: In terms of infrastructure, what component is the most vulnerable, and is that addressed in the NSTIC?

Schmidt: It's really hard to put your finger on what is the most vulnerable. Infrastructure sectors are grappling with the same issues as everyone else: reducing vulnerabilities and preventing disruptions. While we talk about the NSTIC mostly in terms of trying to address identity theft and fraud, there is another important aspect: increasing trust for individual devices. As we move to a more networked world, mobile devices—whether cell phones or smart meters or some new technology—will be working automatically all of the time. How do we make sure those devices are trustworthy? This is just one small piece; there are a lot of moving parts. WA