Testimony of

Dr. Seymour E. Goodman
Professor of International Affairs and Computing
Georgia Institute of Technology

Before the
Subcommittee on Research and Science Education
House Committee on Science and Technology

June 10, 2009

Mr. Chairman, Ranking Member Ehlers, and distinguished members of the Subcommittee: Thank for you for the opportunity to appear before you today to discuss the subjects of Cyber Security R&D and Education.

I am Professor of International Affairs and Computing at Georgia Tech, where I Co-Direct two centers: the Georgia Tech Information Security Center and the Center for International Strategy, Technology, and Policy. I also serve, or have recently served, as chair of the National Research Council Committee that authored *Toward a Safer and More Secure Cyberspace* in 2007; as Vice-Chair of the Institute for Information Infrastructure Protection (I3P), a research consortium of 27 universities, national labs, and federally funded nonprofits; and as the Principal Investigator for Georgia Tech's NSF-funded Scholarship for Service Program.

A large fraction of the American people, its businesses, and government institutions have become increasingly dependent on networked information technologies. We are at risk because these infrastructures are riddled with vulnerabilities and cannot be fully trusted, and there are malicious people who are greatly enabled by network connectivity seeking to exploit those vulnerabilities. Cybersecurity must be viewed as a broad societal issue, in part because vulnerabilities in the general commercial or home computing environments have profound consequences for the vulnerability of many prominent or critical targets. It must also be recognized that cyber protection will be an ongoing need, requiring continually improved responses to dynamically changing circumstances.

These responses will require better and larger education and research programs, and the effective and broad deployment of the output of those programs in timely ways. Technical progress will be of critical importance, but not in itself sufficient. Policy, economic, and behavioral issues must also be addressed. In particular, as discussed in the NRC report, market forces have failed to provide the nation with a

level of cybersecurity adequate for its needs. An authoritative interdisciplinary research study on how this may be changed could be of enormous benefit to the nation. We must also ensure that federally supported research has a broad impact on current and future security challenges. The 2007 NRC report, and the recently released NRC report *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* both note that much of cybersecurity research is classified, and thus unlikely to have much impact in improving civilian security.

I would like to address two particular subjects of both near and long-term urgency and importance. The first is what I fear is a coming tsunami of insecurity due to the spread of cellular telephones and other mobile devices that contain substantial computing capabilities. The second addresses difficulties and progress with efforts to build the capacity to educate a professional workforce that is necessary to help achieve a safer and more secure cyberspace.

The ubiquitous spread of cell phones and other small, increasingly powerful computers with wireless connections is likely to result in unprecedented opportunities for criminals, hackers, terrorists, industrial spies, foreign intelligence agencies, and other unfriendly actors. Cell phone users currently number over 3.5 billion, a majority of the world's population, and vastly outnumber traditional Internet users, especially in developing nations. And cell phone use is growing faster than Internet use. In the next 5-10 years, most of the people on the planet will likely be using powerful mobile devices for more personal and professional functions. And these devices may supplant desktop and laptop computers as the primary form of access to a much larger Internet.

This is leading to increased possibilities for information insecurity, not least because of the huge increase in the number of connected potential malicious actors and potential victims. Forms of attack currently employed against desktops and laptops will be deployed against mobile devices. In addition, there are many vulnerabilities more specific to them, because of battery limitations, the use of airwaves instead of wires, the ease with which they and the information on them may be lost or stolen, particular forms of denial of service attacks, and new and attractive target applications like digital wallets and pocket ATMs.

The vulnerability of mobile devices potentially affects almost every American citizen and organization. Its international dimensions are without precedent. Any research, development, and deployment effort to improve security will necessitate solutions to a large number of interdependent technical and business problems, will require researchers from multiple disciplines, and will depend on strong forms of involvement with the private sector and international institutions to ensure effective and widespread implementation.

So we have warning of looming security problems in a rapidly expanding domain. We have lots of experience and mistakes with the Internet. This time, will we be able

to get ahead of the problem and make the world of mobile cyberspace safer and more secure before the Tsunami forms, builds momentum, and hits us?

A safer and more secure cyberspace will also require many more professionals in the workforce on the front lines defending organizations and infrastructures. To produce these people, we need to increase the capacities of a wide spectrum of educational institutions, adding capable faculty and extensive new curricula, neither of which can be created overnight.

I want to draw your attention to one of the few efforts to grow this workforce on a national scale: the National Science Foundation Scholarship for Service Program (SFS). This program provides some support for universities to build their faculty and curriculum to enable the offering of concentrations in information security and assurance. It primarily provides up to 2-year scholarship support to U.S. citizens in the best of these programs who must (although most see it as an opportunity, rather than an obligation) work in the federal government for at least the same number of years as they were supported by the scholarship. For embryonic information security programs many universities find that these students help provide a critical mass for enrollments for several early years. Graduates help improve the security of the government's information systems and the agencies that depend on them, but more broadly these programs, once established, graduate others who work elsewhere to improve security postures.

The results of this modestly funded program (recently on the order of $10 million per year) have been impressive. Since 2003, 970 mostly MS-level professionals from 34 universities across the country have been placed in agencies. Many programs at these universities may not have become viable without the NSF support, and the majority of the scholarship students would not have chosen to study cybersecurity and work for the federal government without the visibility and inducements of the program. Some of these universities have become assets to other regional educational institutions, including schools for law enforcement and 2-year colleges.

Most of the curriculum being developed and offered is in the form of computer science courses. These are necessary, but not sufficient, to the educational needs. There is a need for multidisciplinary courses that introduce important matters relating to management, law, policy, human behavior, and the international dimensions of cybersecurity. Only a small number of universities have serious courses of this kind. They should be designed with the intention of facilitating export to many institutions since few have faculty in positions to work on these aspects at this time. Perhaps an NSF program might help address such needs?

The government has done well in establishing this program, to its own direct benefit and the country's more generally. It should be continued and carefully augmented to have a more extensive impact. Thoughts along those lines might include the range of degrees supported with the scholarships, and the range of employment options

permitted, for example, teaching at 2-year colleges or in parts of the country with particular needs.

A major capacity building bottleneck that affects all levels of educational and research needs is the production of PhDs in this area. Today, at most levels of tertiary education, a PhD is a necessary credential for a long-term career. Many who are working these problems as researchers and educators are recent additions to the ranks, as newly minted PhDs or converts from other fields. Building the doctoral ranks takes time and others who can provide close supervision. However the task is not insurmountable; it will take a concerted effort that should be pursued with national-level vigor.

This concludes my statement. I will provide some additional written material to the Subcommittee's staff.

Thank you for inviting me to testify. I would be happy to try to take any questions you have.

Biographical Sketch

Seymour (Sy) E. Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of the Center for International Strategy, Technology, and Policy and Co-Director of the Georgia Tech Information Security Center.

Prof. Goodman studies international developments in the information technologies and related public policy issues. In this capacity, he has over 200 publications and served on many academic, government and industry advisory, study, and editorial committees. He has been the International Perspectives editor for the *Communications of the ACM* for almost 20 years, and has studied computing on all seven continents and in about 90 countries. He recently served as Chair of the Committee on Improving Cybersecurity Research in the United States, National Research Council, Computer Science and Telecommunications Board, National Academies of Science and Engineering.

Immediately before coming to Georgia Tech, Prof. Goodman was the director of the Consortium for Research in Information Security and Policy (CRISP), jointly with the Center for International Security and Cooperation and the School of Engineering, Stanford University. He has held appointments at the University of Virginia (Applied Mathematics, Computer Science, Soviet and East European Studies), The University of Chicago (Economics), Princeton University (The Woodrow Wilson School of Public and International Affairs, Mathematics), and the University of Arizona (MIS, Soviet and Russian Studies, Middle Eastern Studies).

Prof. Goodman was an undergraduate at Columbia University, and obtained his Ph.D. from the California Institute of Technology where he worked on problems of applied mathematics and mathematical physics.