Written Testimony of

Dr. Frederick R. Chang

President and COO

21CT, Inc.

Before the

Subcommittee on Technology and the Subcommittee on Research

Committee on Science, Space and Technology

U.S. House of Representatives

Hearing on

"Cyber R&D Challenges and Solutions"

February 26, 2013

Chairman Massie, Chairman Bucshon, Ranking Member Wilson, Ranking Member Lipinski, Members of the Committees, thank you for the opportunity to testify before you in today's hearing on the topic of *Cyber R&D Challenges and Solutions*. My name is Frederick R. Chang and I am currently the President and COO of 21CT, Inc. in Austin, Texas. In prior positions, I have served at the National Security Agency (as Director of Research); in academia (at The University of Texas at San Antonio and at The University of Texas at Austin); and in the telecommunications industry (at SBC Communications, Pacific Bell, and Bell Laboratories). I would also mention that I have served as a member of the CSIS Commission on Cybersecurity for the 44th Presidency and I am currently a member of the Texas Cybersecurity, Education, and Economic Development Council.

You may not have heard of my company 21CT, Inc. before, but briefly we are a small, technology company headquartered in Austin, Texas. We have a 12-year history of maturing

new technologies, starting with early research and going all the way through operational military and commercial use. Our products are focused on the areas of intelligence analytics, computer network defense analytics, and fraud detection.

The Cybersecurity Challenge

Not too long ago, we were anxiously awaiting the arrival of the "Information Superhighway". It promised to improve our productivity, enrich our lives, educate our children and so much more, via e-commerce, e-banking, e-learning, e-government, and the like. The Internet and the world-wide-web are among the most successful technological and commercial advances in human history. Yet with all the progress and success, there is a dark cloud hanging over cyberspace, and that dark cloud is security. Cyber infrastructure is tightly woven into the very fabric of our lives and it would be very hard to imagine going back to an earlier time -- but we are paying a heavy price for our technological dependence and the problem is worsening with the passage of time. Our trust in cyberspace has been taken from us by hackers, cybercriminals and sophisticated cyber attackers who intend to do us harm. We deserve better. We expect our information to be confidential from prying eyes. We expect system resources to be available to us if we are legitimate users of those resources. We expect that our information will not be altered in a way that we do not intend. We expect that it should not be impossibly difficult to protect ourselves in cyberspace if/when the need arises. These expectations are simply not being met today. Attacks on both the public sector and the private sector are rampant. Denial of service, identity theft, and cyber extortion are now all too common. As you are all abundantly aware, financial systems, national critical infrastructure systems, defense systems, and much more are all targets of sophisticated cyber attacks.

Science of Cybersecurity

The discipline of cybersecurity today is too reactive and after-the-fact. In general, something bad has to happen and then action is taken. There is certainly some ability to stop things that have been seen before, but unfortunately new attacks, that haven't been seen before, are all too common. Cybersecurity is not based on a firm science and engineering foundation and I believe it is critically important that such a foundation be created. Some important activity has started along these lines [e.g., 1, 2], but much more is needed. In our school science classes we learned that water at sea level changes from a liquid into a gas at 100 degrees Celsius and into a solid at 0 degrees Celsius. Similarly we learned about gravity and that a freely falling object near the earth's surface will increase by approximately 9.81 meters per second every

second. In science, the notions of laws, principles, experiments, metrics, repeatability, and predictability (among others) are commonly used. These words and ideas are not common in discussions of cybersecurity today, unfortunately. Indeed it has been noted [3] that when it comes to predictability, about the only thing we can predict confidently in cybersecurity is that a sufficiently motivated attacker will be able to compromise the targeted system.

There are at least three different ways to think about the role of science in cybersecurity [4, see also 5]:

1) Universal laws that enable strong quantitative predictions;
2) Systematic generalizations of knowledge;
3) Conduct of research through hypothesis formation and experimentation.

While progress is being made, we have much more work to do in all three areas.

Cybersecurity metrics

"If you can not measure it, you can not improve it."

"I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science*, whatever the matter may be."*

These quotes are from the influential 19th century mathematical physicist and engineer Lord Kelvin, and are appropriate in a discussion of cybersecurity metrics. While important work is taking place [e.g., 4], we need improvements in hard, objective metrics and measures of security. Metrics are needed at many very practical levels. At a very tactical level, how do you know if computer system A is more or less secure than computer system B? Is computer system A more secure than it was last month? Last year? At a corporate level, how you do measure the security of your corporate information technology infrastructure? Is it more secure now than it was last year? Do the measures allow a pinpoint assessment of where corporate improvements are necessary? At a much more macro level, what metrics are best used to determine if the industry as a whole is making progress toward improving its cybersecurity posture? How would you measure the effect of an important government policy change in

cybersecurity? Is it making the difference that was intended? It is relatively straightforward to determine the effects of changing the speed limit on traffic accidents. It won't be so clear for cybersecurity. Developing a disciplined, agreed-upon, and readily implementable set of metrics for cybersecurity remains a hard problem. Perhaps we can look for some assistance from other fields -- medical research has successfully employed metrics to improve the science of human health. Measures of human health and cyber health share an important common ingredient: in both cases we are attempting to measure the absence of something bad (human disease or system compromise).

Cybersecurity Research and Development

In the December 2008 report from the CSIS Commission on Cybersecurity for the 44th Presidency [6], we estimated that in 2009 about 0.2% of federal R&D funding would go into cybersecurity. That was several years ago, and no doubt the picture is different today, but at least as of that time, we start from a very small base. Let me highlight just a few areas that I think are important in addition to the science of cybersecurity thrust mentioned previously.

Psychology and security

While travelling in London some years ago, I was nearly pulverized by one of those large red double-decker buses. Being from the United States, before crossing a street, I am accustomed to looking to my left before crossing. In this case, this instinct did not serve me well. I believe that something similar is occurring for many people as we make decisions and operate our computers in cyberspace. The instincts and tendencies that serve us well, the vast majority of the time in the physical world actually betray us in the complex, abstract, virtual world of cyberspace.

Security is very often about the weakest link. Hackers need just one way in. As technical security measures improve (e.g., greater use of encryption), then people increasingly become the weakest link. Hackers often employ a tactic known as "social engineering" to trick computer operators to divulge sensitive information that can be used to compromise a system (e.g., a password). These tactics can be extremely effective and much easier to accomplish than a technical compromise. Indeed the well-known hacker Kevin Mitnick reported in testimony to Congress that he was so successful in social engineering that he rarely had to resort to a technical attack [7]. More generally, there are a well-known set of cognitive biases that people use to assess risk and make decisions [8]. These biases often cloud our reasoning and cause

us to improperly assess risk, in many domains, including in cyberspace. We must take steps to strengthen the weakest link. Gaining a much richer understanding of the cognitive biases at work in the context of decision-making in cyberspace would be just one of many important issues that need research at the intersection of psychology and cybersecurity.

Software assurance

Software is vulnerable – and that is a key reason why cyber compromise is so prevalent today. Modern software systems are exceedingly complex and not only must work correctly in the face of error or mischance, but must also work correctly when an adversary is trying to attack them – and this is exactly the sort of hostile environment that cyberspace creates for software. Software today too often treats security as an after-the-fact problem. The software is developed, tested and released and then a security incident occurs and the software must be patched, after-the-fact. We must move to a model where security is built in to software from the very beginning. How can we make dramatic breakthroughs in methods, procedures, metrics and the like that incorporate building security into software, such that software is built to be inherently resistant and resilient to attack? Can we introduce these new techniques in ways that are cost-effective, that speed time to delivery and that are convenient to use for developers? Can we compose new secure software from component pieces that are not secure? There have certainly been important contributions made in this area of research, but I believe it is time to accelerate and reinforce innovation and progress.

Trustworthy systems

Apparently we don't trust the software on our computers. We have millions and millions lines of software code on our machines in the form of operating systems, device drivers, applications, etc. We know that code may not be secure, so we purchase additional security software in the form of firewalls, anti-virus software, anti-spyware software and the like. Well, security software may be vulnerable as well, so now what? Do we buy a firewall for our firewall? You get the idea. Related to the software assurance topic above is the notion of the need to build systems that are inherently trustworthy. The problem expands in scope rather dramatically when you now must consider building scalable trustworthy systems; systems of systems connected by networks that must all be inherently trustworthy. You want these systems and networks to be highly available, highly reliable, highly resilient, etc. These are very hard problems that will defy easy solution as systems and networks continue to grow in size, scope and complexity.

Economics and cybersecurity

Would you spend $50 on software to help protect my computer? When you purchase anti-virus software for your computer, one of the things that it is supposed to do is help ensure that your computer does not become part of something called a botnet. If your computer becomes a bot, this would mean that unwanted, malicious software has been installed on your computer that allows a hacker (also called the botmaster) to take control of your computer. Once the botmaster has seized control of your computer he/she can command it, for example, to do malicious things to other computers – perhaps mine. So in a very real way, the security of my computer depends on whether or not you have purchased software to protect your computer. It is important to note that this has nothing to do with technology per se but rather with whether economic incentives are in alignment. That is to say, the security of a system may have more to do with economic incentives than with technical capability. Similarly, software companies are capable of making their software more secure but so far they haven't been economically incented to do so. Business factors such as speed to market, enhanced features, improved system performance, and the like, often take priority over security. How much should a firm spend to secure its cyber infrastructure? Does increased spending on cybersecurity result in improved cybersecurity? How should the money be spent? On hardware or software or more staff? What about a cybersecurity insurance policy? Research here will be related to work on metrics. An active field of research has been started in this area – the results are most illuminating -- and much more is needed.

Cybersecurity as a "wicked problem"

In May of 1961 President Kennedy announced a bold national goal, "before this decade is out, of landing a man on the Moon and returning him safely to the Earth." As we all know, that historic mission was successfully accomplished in July of 1969. Early computer security work was starting at around the time Apollo 11 was splashing down in the Pacific Ocean, and now – well over 40 years later – computer security is far from a solved problem. Why has this been so hard? There are many reasons, but recently people have talked about cybersecurity as a "wicked problem" [9]. Wicked in this context does not refer to evil, but rather resistance to solution. Wicked problems are extremely difficult and perhaps impossible to solve and include these properties, among others [10]:

1. The problem is not understood until after the formulation of a solution.

2. Wicked problems have no stopping rule.
3. Solutions to wicked problems are not true-or-false, but rather better-or-worse.
4. Every wicked problem is essentially unique.
5. Every solution to a wicked problem is a 'one shot operation'
6. Wicked problems have no given alternative solutions.

To the extent that cybersecurity is indeed a wicked problem, then I believe that an interdisciplinary research approach is needed. In addition to the disciplines of psychology, computer science and economics described above, what can we learn from the fields of biology, medicine, physics, anthropology, political science and more? I believe these other disciplines will add much to the research dialogue.

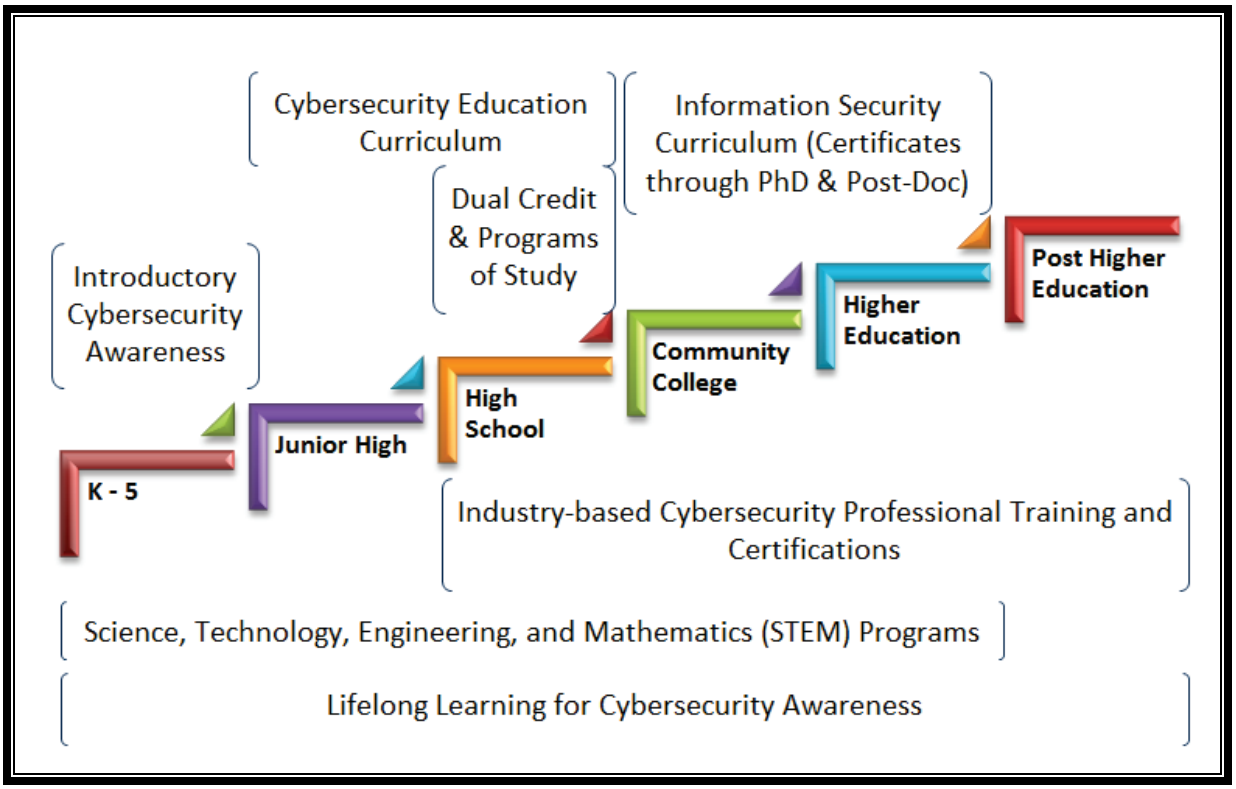
There are other important research topics that are not described here, that are worthy of mention including: secure cloud computing, secure mobile computing, secure hardware, secure hypervisors, secure coding, insider threat, data science, and many more.

The Cybersecurity Skills Gap

"The cyber threat to the United States affects all aspects of society, business and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the federal government."
(Source: Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity for the 44th Presidency, *Dec. 2008.)*

The cybersecurity skills gap has been discussed extensively over the last few years [e.g., 11] and indeed the continuing shortage of qualified cyber professionals remains a major obstacle in making significant progress in cybersecurity. Representing a small company with on-going demands for highly technical cyber hires, it is a constant challenge for us to identify and recruit the necessary expertise – and this is a consistent theme.

In our work on the Texas Cybersecurity, Education and Economic Development Council [12], the skills gap issue came up time and time again. It was clear to us that the workforce gap would be a long-term problem and we advocated a "pipeline" approach to ensure a long-term supply of well-trained, motivated cybersecurity professionals in the state. This K-through-PhD approach is represented in the figure below and incorporates both professional training and awareness training.



Proposed Texas Cybersecurity Education Pipeline

(Source: Texas Cybersecurity, Education, and Economic Development Council, Dec. 2012)

In addition to a broad-based "pipeline" approach, I believe it is extremely important to take a depth-based view as well. "There are about 1,000 security people in the US who have the specialized security skills to operate at world-class levels in cyberspace. We need 10,000 to 30,000" [11]. This quote is reflective of the fact that while there is a broad and long-term skills gap, the gap is especially large when it comes to the exceedingly deep technical knowledge needed to operate at the highest level. For example, in compromising a system, a sophisticated cyber adversary will do so in a way that avoids detection. Thus to detect the compromise requires a very high level of skill. A national discussion of the cybersecurity skills gap must include innovative ideas as to how to increase substantially the number of cyber professionals with exceedingly deep technical skill.

Comments on H.R. 2096, The Cybersecurity Enhancement Act of 2012

I was asked to comment on H.R. 2096, The Cybersecurity Enhancement Act of 2012, and would offer these brief comments:

1. There is considerable mention of cybersecurity workforce issues in this legislation: training, education, awareness programs, scholarships, and the like. As mentioned previously, the cybersecurity skills gap today is large and represents a major obstacle to significant progress in improving the nation's cybersecurity posture. Initiatives that lead to breakthrough progress in the skills gap are to be applauded. I would note the point I mentioned previously in my testimony regarding the especially large skills gap when it comes to the numbers of people possessing exceedingly deep technical skill and would encourage particular attention in this area. Let me also say that while in academia I had the opportunity to witness the benefits to students of programs like the NSF Scholarship for Service Program and the Department of Defense Information Assurance Scholarship Program. These scholarships are making a difference and I believe they are an important tool in helping to close the nation's cybersecurity skills gap.
2. In section 109 of the legislation there is discussion of the need for security automation and continuous monitoring. These are both important concepts and critical at this time as cyber adversaries will continually adapt their attack vectors, in an effort to thwart the current defensive posture that is in place. I believe it is important to automate what you can, but hasten to point out that, as we all know, automation can never be perfect – something will get through. That leads us to continuous monitoring, which is similarly important, but I would add that there needs to be some consideration given to requiring continuous improvement along with continuous monitoring. We should have the expectation that the networks that are being continuously monitored, become increasingly more resilient over time, as well.
3. Finally, a centerpiece of this legislation is cybersecurity research and development. I mentioned earlier in my testimony the estimate of 0.2% of federal R&D spending going to cybersecurity R&D in 2009. I believe that older estimate is worth repeating here because to the extent that this legislation can raise the trajectory of cybersecurity R&D spending from its historical levels, that would create long-term benefit in our effort to improve the nation's cybersecurity posture. In my testimony I also highlighted the importance of social science research (in psychology and economics, in particular) and indeed social science research and cybersecurity are specifically identified in Section 104. In Section 108 there is a discussion of a cybersecurity university-industry task force to explore opportunities for collaboration in research, development, education and training. As part of those task force deliberations, I believe it would be valuable to have some discussion about the task force potentially creating and then issuing some

cybersecurity research grand challenges – that meet the needs of industry, government and academia. Solutions to such grand challenges could help advance the field and at the same time help solve some enduring hard problems facing practioners in the future. Finally, and more generally, in my testimony I stressed the importance I place in developing a science of cybersecurity. I would mention here that not all cybersecurity research produces a benefit to cybersecurity science. It's a subtle but important point. Among other things, cybersecurity science should tell us something about the limits of what is possible in a particular security domain, and have broad applicability beyond a specific platform, a particular attack or a certain defensive implementation. To be sure, increasing the amount of very high-quality cybersecurity research will produce a tangible benefit, but it would be my hope that some of that high-quality research be directed toward advancing the science of cybersecurity.

Let me close by saying that I've suggested some items in my testimony that will take a long time to implement. For example, producing a long-term, robust and deeply technical cybersecurity workforce or creating a science of cybersecurity, could take decades. I'm reminded of an old proverb: The best time to plant a tree was 20 years ago – the second best time is now. Thank you again for giving me the opportunity to speak to you today.

References

1. JASON Program Office. Science of cyber-security. Report No.:JSR-10-102. The Mitre Corporation, McLean, VA, November 2010.
2. Developing a blueprint for a science of cybersecurity, The Next Wave, Vol. 19, No. 2, 2012, National Security Agency, Ft. Meade, MD.
3. Evans, D. & Stolfo, S. The science of security. *IEEE Security & Privacy,* **9**, 16-17, 2011.
4. Stolfo, S., Bellovin, S.M. & Evans, D. Measuring security. *IEEE Security & Privacy,* **9**, 60-65, 2011.
5. Schneider, F.B. Blueprint for a science of cybersecurity, The Next Wave, Vol. 19, No. 2, 47-57, 2012, National Security Agency, Ft. Meade, MD.
6. CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, Center for Strategic and International Studies, Washington, DC, December 2008.
7. Mitnick, K. Kevin Mitnick in a hearing before the Committee on Governmental Affairs, U.S. Senate, "Cyber Attack: Is the Government Safe?" March 2, 2000.
8. Kahneman, D., *Thinking, fast and slow.* Farrar, Straus and Giroux, New York, 2011.
9. Lucky, R.W. Cyber Armageddon. *IEEE Spectrum*, vol. 47, no. 9, pp. 25-25, 2010.
10. Rittel, H. & Webber, M. Dilemmas in a General Theory of Planning, *Policy Sciences*, **4,** 155–169, 1973.
11. A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. CSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, Washington, DC, July 2010.
12. Building a More Secure and Prosperous Texas: A Report from the Texas Cybersecurity, Education, and Economic Development Council, Austin, TX, December 2012.