Written Testimony of

Dr. Frederick R. Chang

Executive Director, Darwin Deason Institute for Cyber Security

Southern Methodist University

Before the

Cybersecurity and Infrastructure Protection Subcommittee

Homeland Security Committee

U.S. House of Representatives

Hearing on

"Challenges of Recruiting and Retaining a Cybersecurity Workforce"

September 7, 2017

Chairman Ratcliffe, Ranking Member Richmond, Members of the Subcommittee, thank you for the opportunity to testify before you in today's hearing regarding the challenges associated with recruiting and retaining a cybersecurity workforce. My name is Frederick R. Chang and I consider it an honor and a privilege to come before this Subcommittee. I am the Executive Director of the Darwin Deason Institute for Cyber Security at Southern Methodist University (SMU) in Dallas, Texas. I am also the Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Professor in the Department of Computer Science and Engineering in SMU's Lyle School of Engineering, and a Senior Fellow in SMU's John G. Tower Center for Political Studies. Prior to coming to

SMU, I have held academic positions at the University of Texas at San Antonio and at the University of Texas at Austin. I have worked in the private sector and have also served as the Director of Research at the National Security Agency. I would also mention that I served as a member of the CSIS Commission on Cybersecurity for the 44th Presidency.

SMU is a nationally ranked private university in Dallas founded over 100 years ago. The university enrolls more than 11,000 students - including about 5,200 graduate students - who all benefit from the academic opportunities and international reach of seven degree–granting schools. The Carnegie Foundation recognizes SMU as a university with “high research activity," which ranges across disciplines from particle physics at the Large Hadron Collider at CERN, to geothermal energy, to the science of human speed, to cyber security through the Bobby B. Lyle School of Engineering. SMU’s Lyle School of Engineering, founded in 1925, is one of the oldest engineering schools in the Southwest. The school offers eight undergraduate and 29 graduate programs, including master’s and doctoral degrees, through the departments of Civil and Environmental Engineering; Computer Science and Engineering; Electrical Engineering; Engineering Management, Information, and Systems; and Mechanical Engineering. Finally, the Darwin Deason Institute for Cyber Security is a research institute with the goal of advancing the science, policy, application and education of cybersecurity through basic and problem-driven, interdisciplinary research.

The New Normal

Early computer worms and viruses date back to the 1970’s and 80’s and while they were rare and experimental back then, as we fast forward to 2017, terms such as “malware”, “data breach”, “phishing” and “botnets” are unfortunately all too common today. We are no longer surprised to read about the latest data compromise or cyberattack as they are sadly a regular occurrence. In fact, not long ago a technology company ran a series of television commercials depicting that it is newsworthy when there is not a data breach. The Internet, high-performance computing clusters, high-density storage, ultra high-speed communication links, the cloud, our laptops and smart

phones are technologies that we take for granted today. They are so integral to our personal and professional lives that it is hard to remember a time when we didn't have these technologies available to us. But in the larger scheme of things the technologies that comprise cyberspace are young and changing at a stunning rate of speed. As we have become increasingly dependent on these technologies we have also come to understand just how vulnerable these technologies are to malicious attackers of many kinds. We have also come to understand the consequences of these security vulnerabilities to us personally, professionally, and to our national security.

The source of today's cyber insecurity is multifaceted involving, technology, policy, law, economics, workforce, and more. In my brief comments this afternoon, I will focus on the topic of today's hearing: the cybersecurity workforce. One of the reasons why cyber intrusions are so prevalent today is that there is a lack of trained, qualified personnel to defend the nation's cyber assets. This lack of trained personnel has been referred to as the "cyber skills gap".

The cyber skills gap

Over the past several years there has been increasing concern about the cyber skills gap problem, and the extent to which this gap contributes to the nation's challenge in defending cyberspace, today and into the future. An image that comes to mind is from the child's game of whack-a-mole. Cyber defenders within an enterprise are stretched too thin, quickly moving from issue to issue in an effort to keep their networks secure. Two natural questions to ask are: How large is the problem? Is the problem going to get worse in the future? There have been a number of studies and reports on this topic and I have listed a few illustrative bullets points below that shed some light on these questions. I would hasten to add that perhaps more important than the specific numbers that are listed are the trends that they suggest.

- The size of the global cyber skills gap was estimated at about 1 million people in a 2014 report [1, see also 2].
- The size of cyber skills gap globally will grow to about 1.8 million in 2022. This is 20% higher than an estimate made two years earlier [3].

- The size of the cyber skills gap in the U.S. was estimated to be over 200,000 in 2015 [4]. The size of the cyber skills gap is estimated to grow to about 265,000 in North America by 2022 [3].

- In the United States there were nearly 300,000 on-line job listings for cybersecurity-related positions between April 2016 through March 2017, and the national average ratio of existing cybersecurity workers to cybersecurity job openings is only 2.5, while the national average for all jobs is 5.6 according to the website CyberSeek [5].

In addition to the shortfall estimates above, it is instructive to look at some illustrative responses sampled from a variety of different surveys of different groups of cybersecurity professionals. The goal here is not to be exhaustive but rather to provide a perspective on some of the challenges facing enterprises as they address the challenges associated with hiring qualified cybersecurity workers.

In one international survey, the North American respondents reported that they were not able to fill open cybersecurity positions about 26% of the time and that for all respondents, over a quarter of the time finding an appropriate person for the job can take up to 6 months. In the same survey, respondents reported that while they do receive quite a few applicants for each job opening, most applicants are viewed as unqualified – and this response is reflected by the North American respondents to the survey as well [6].

In another survey that included only North American respondents (Information Technology (IT), and IT security professionals), 35% reported that there is a shortage of IT security professionals at most every level, and 37% reported that there are lots of less experienced/trained people, but it is hard to fill the most-skilled positions. In the same survey only 33% of respondents report that they have enough people to meet the threats they will face in the coming year and only 23% report that their security team is well trained and up-to-date on the latest technologies and threats [7].

In a study we conducted at SMU we explored how organizations made cybersecurity investment decisions [8]. We conducted semi-structured interviews with cybersecurity

executives and managers from primarily four vertical sectors: healthcare, financial, retail and government. Over 75% of the respondents were from U.S. organizations. Consistent with the findings reported above, our respondents reported that finding qualified cybersecurity talent was a key challenge. Sufficient budgets were often available for a particular cybersecurity project but that lack of availability of qualified personnel served as a limiting factor in budget requests. Respondents reflected that even though they had considerable professional networks from which to draw, they had difficulty finding the talent they needed.

Finally, a theme that was highlighted in one of the earlier reports on the cyber skills gap emphasized the need for technical talent. Indeed this need is reflected in the report title: *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters* [9]. A quote from the report describes the sentiment well: "We not only have a shortage of the highly technically skilled people required to operate and support systems we have already deployed; we also face an even more desperate shortage of people who can design secure systems, write safe computer code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute systems after an attack".

Cyber students in demand

The previous section provided some perspective on the size and nature of the cyber skills gap today and into the future and the trends are that the gap is large and challenging today and that it will worsen in the years ahead. As enterprises think through how they will staff to meet their cyber defense needs they will do well to think creatively and unconventionally as talent could well come from disciplines that are not traditionally associated with cybersecurity. Additionally, as cybersecurity becomes a higher priority within an enterprise, talented employees from different parts of the enterprise can and are being retrained to move into higher priority cyber positions. In fact, we've offered an MS degree in Security Engineering for over a decade at SMU and that degree is popular with corporate employees who are interested in retraining themselves.

For an enterprise it is clearly desirable to be able to hire highly experienced professionals who can immediately perform at a high level, but due to the talent shortage and associated salary limitations that may not always be possible. An alternate strategy may be to strategically hire more junior talent and patiently grow the needed capability internally. Indeed in our own research [8] some of our respondents expressed this perspective. So, in addition to the natural course of hiring college graduates for positions that are appropriate for their skill level, there is additional demand for cyber-capable college graduates. I am seeing this demand for our students at SMU as are my peers around the country for their students at their respective universities.

As part of our undergraduate computer science major, we've offered a security track for many years now in which students can take elective courses in security which allows them to emphasize cybersecurity as part of their undergraduate computer science major. We are seeing an uptick in the number of students who are pursuing this security track and we believe that when students pursue this track they very often go on to pursue a cybersecurity-related job upon graduation. In addition, anecdotally, we are seeing an uptick in the number of high-school seniors who plan to pursue cybersecurity in their undergraduate studies.

Answering the need

The cyber skills gap has been known about and discussed for many years now and over time, I've had my fair share of discussions with enterprise managers who are eagerly awaiting the arrival of more trained cyber defenders. As mentioned above these students are in high demand. While for many hiring managers the supply of students isn't arriving fast enough to meet the demand, there are many activities underway in the government, the private sector, and academia – often working together – that are helping to meet the demand. Let me touch on a few such activities below.

Centers of Academic Excellence and Scholarships. Historically the NSA/DHS Centers of Academic Excellence in Cyber Defense (CAE-CD) program (and extensions) have helped to jump start skill building in cybersecurity in higher education, by among other things, requiring the CAE-CD designated universities to map their curriculum to specific

information assurance knowledge units. Additionally the government has funded scholarship programs (the NSF CyberCorps® Scholarship for Service, and the Department of Defense, Information Assurance Scholarship Program) that have provided funding (tuition, books, stipend, etc.) for students to complete their cybersecurity education in return for service to the government following graduation.

Curricular guidance. As more university capability, capacity and programs are created to answer the need for more cyber defenders it will be important to have clear curricular guidelines that will assist in building these new programs. Cybersecurity is still a young field but is emerging as a distinct discipline. As universities compose new cybersecurity academic programs out of elements from computer science, computer engineering, information systems and the like, it will be extremely valuable to have comprehensive curricular guidance. The ACM (Association for Computing Machinery) Joint Task Force on Cybersecurity Education is in the process of creating this guidance and it is expected to be released later this year [10]. Importantly it defines cybersecurity as an interdisciplinary area of study including elements from risk management, policy, human factors, law and more, but that fundamentally is a computing-based discipline.

Cyber Competitions. For over a decade now university students have been competing in a cybersecurity competition that is now known as the National Collegiate Cyber Defense Competition (NCCDC). The competition provides a challenging and motivating event in which students must defend a simulated small company network while operationally keeping services up and running while responding to business requests. Depending on how they do, points are scored and teams advance in the competition. The competition has grown in popularity over the years and now there are 10 regions across the country that compete, and the regional winners compete in a national finals event. At the national finals event, a national winner is crowned. Cyber competitions in general have become very popular, and there are now many in which to participate and they focus in different areas (cybersecurity, forensics and capture-the-flag). With the increasing number of cyber competitions it is fair to ask about their educational impact [e.g.,11]. That said, cyber competitions provide a means to increase depth of technical knowledge in cybersecurity [12] and there is some evidence that cyber competitions will attract individuals who will stay in the field a long time [13]. At SMU there is a student

run security club where interested students meet to learn from each other and practice security concepts. A highlight for club members is to participate in cyber competitions including the NCCDC. The cyber competitions are popular with the students in part because they feel the competitions provide a valuable supplement to what they learn in class. Additionally, cyber competitions give students experience working as part of a team, and this is valuable when they graduate and join the workforce. As the popularity of cyber competitions has continued to grow, they have moved into the K-12 domain as well.

Cyber summer camps. Related to, but distinct from cyber competitions, are summer cybersecurity camps for K-12 students. For example, the GenCyber program, funded by NSA and NSF, offers a summer cybersecurity camp experience to middle and high school students, as well as teachers, in an effort to increase the pool of students who might go on to study cybersecurity in the United States. One of the goals of these summer camps is to teach students about cyber safe and correct on-line behaviors. Over the last several years, in keeping with the effort to get more K-12 students interested in the STEM (Science, Technology, Engineering and Math) fields, among other things, SMU has conducted a Crime Scene Investigation (CSI) summer camp for middle schoolers. Students are introduced to the science, technology and math behind CSI via expert presentations from real-world professionals and hands-on activities. For the past two summers we have added a cybersecurity module into the CSI curriculum.

Augmenting human capability with technology. Finally, there are some important efforts to augment human capability in cybersecurity via the use of technology. For example, there is promise in the use of advanced reasoning techniques to augment the human cyber expert by automating some portions of the cyber defense task (e.g., finding and fixing flaws in software). This was the goal of the recent DARPA Cyber Grand Challenge in which important advances were made in the ability to automate the process of detecting software vulnerabilities, creating an appropriate patch, and then applying that patch in real-time [14]. To the extent that these, and other, difficult and time-consuming tasks can be automated, this will leave the time-limited human cyber expert more time to perform important analytic tasks that are not able to be automated at this time.

Conclusions

Many students I speak with are eager to join this new field and as mentioned previously we are seeing an uptick in that interest. I occasionally engage students in brief career-oriented discussions and a few themes emerge in these discussions as students think about their job choices that I thought might be relevant as we discuss recruiting and retaining top cyber talent.

1. The students want challenging work. They are challenged in their coursework to master difficult technical material, but also exercise creativity in using those skills. They want nothing less when they move into the workplace. They want to jump into the game and show that they have what it takes.

2. The students want to make a difference. As they evaluate positions they will try to determine if the position will allow them to make a difference – they want their efforts to have an impact. Sure, salary will be a factor, but as one student commented, for some they will choose “mission over money”.

3. The students want to keep their technical skills sharp. When students graduate their technical skills are sharp and up to date. They understand that the computing and technological landscape changes rapidly. They will want to work with the most modern tools, with colleagues who they respect and from whom they can learn, and in an environment that gives them opportunities to refresh their technical skills.

In closing, in my comments earlier I briefly mentioned a number of activities that the nation is undertaking now in an attempt to help close the cyber skills gap including: scholarships, new cybersecurity curricular guidance, cyber competitions, cyber summer camps, and technological advances that will augment human cyber capability. These activities are important, valuable, and are making a difference, but I believe we can and should do more. We now have a much better understanding of the constantly changing nature of the cyber threat and the consequences of our cyber insecurity. Are there lessons to be learned from America’s “Sputnik moment” nearly 60 years ago? Following the launch of the Soviet satellite Sputnik in 1957, science education got an

infusion of funds of over a billion dollars in 1958 when the National Defense Education Act was passed, and this helped launch a new generation of students who would to be motivated to go on to study math and science [15]. The challenge to make cyberspace more secure is a long-term, enduring problem. While we urgently need short-term solutions to make available more cyber-trained workers to fill positions now and in the near-term, we also need to ask ourselves what will cyberspace look like 10, 20 and 30 years from now – and how much more dependent will we be on it? Today's students will be responsible for designing, creating, operating, maintaining and defending tomorrow's cyber infrastructure.

Thank you again for allowing me the opportunity to be here today. I look forward to your questions.

References

1. Cisco 2014 Annual Security Report, Cisco Systems, San Jose, CA, 2014.
2. Cobb, S. Sizing the Cybersecurity Skills Gap: A White Paper, 2016. Paper can be found here: http://cisosurvey.org/wp-content/uploads/2016/10/sizing-cyber-skills-gap-v1a.pdf
3. 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, report can be found here: https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf.
4. Setalvad, A. Demand to fill cybersecurity jobs booming, Peninsula Press, March 31, 2015, report can be found here: http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/
5. http://cyberseek.org/heatmap.html
6. State of Cyber Security 2017, Part 1: Current Trends in Workforce Development, ISACA, 2017.
7. Chickowski, E. Surviving the IT Security Skills Shortage, Dark Reading Reports, May 2017.
8. Moore, T., Dynes, S. & Chang, F. Identifying How Firms Manage Cybersecurity Investment. Paper presented at the 15th Annual Workshop on the Economics of Information Security, June 13-14, 2016 Berkeley, California.
9. A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. A White Paper of the CSIS Commission on Cybersecurity for the 44th Presidency, July 2010.
10. https://www.csec2017.org/
11. Fulton, S., Schweitzer, D., and Dressler, J. What Are We Teaching In Cyber Competitions? Frontiers in Education Conference (FIE), October, 3-6, 2012.
12. Manson, D., and Pike, R. The case for depth in cybersecurity education. ACM Inroads, Vol. 5, No. 1, pp. 47-52, March 2014.
13. Tobey, D.H., Pusey, P., and Burley, D.L. Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league, ACM Inroads, Vol. 5, No. 1, pp. 53-56, March 2014.
14. https://www.darpa.mil/news-events/2016-08-04
15. Abramson, L. Sputnik Left Legacy for U.S. Science Education, All Things Considered, NPR, September 30, 2007. Story can be found here: http://www.npr.org/templates/story/story.php?storyId=14829195