Meeting the Cyber Security Workforce Demand

By Drew Hamilton

Mississippi State University

Twenty years ago it was reasonable to think that the demand for computer security would crest as technological innovations secured what we now call cyberspace and our connection points into cyberspace. It was tempting to remember studies cited in the first information systems courses in the sixties showing curves that indicated that eventually every man, woman and child in the United States would need to become switchboard operators in order to meet projected demands. Of course that did not take place – technology replaced the vast majority of human telephone operators.

Currently, new technology is actually *increasing* cybersecurity workforce demands and broadening and deepening the skill sets required for the cybersecurity workforce – quite the reverse from the telephone operator issue. In this short paper, we will consider the following issues:

1. CyberCorps and its impact on the US Civil Service, the private sector and a revived DOD Information Assurance Scholarship Program (IASP)
2. Education versus training
3. New Technology and Cybersecurity education
4. Future Directions

1. CyberCorps and its Impact

The impact that the NSF CyberCorps program has had on the Federal cybersecurity workforce has been well-documented elsewhere. There has also been a positive impact on state, local and tribal governments. In many rural areas, the only way a state or local government entity can make a quality cybersecurity hire is with a Cybercorps graduate who has a service obligation and wants to stay close to home.

Early in the days of the SFS program, some PIs were encouraged to prioritize placements in non-DoD Federal Service. At that time, the DoD IASP was running a similar program, but one where student scholars were selected by the DoD agencies where they were expected to intern and then serve out their service obligations. But the DOD IASP did not consistently produce close to the number of scholarship students as SFS. With rumors of a revival of the DoD IASP, it may make sense for the DoD program to specialize in DoD-unique and mostly DoD-unique cybersecurity skills such as attack, exploitation and intelligence tradecraft.

While SFS has clearly impacted the Federal workforce, it has also had a major impact on the US private sector workforce. SFS enabled its Federal sponsors to "lock up" the best student talent early and commit them to government service. Industry has paid attention. Tech firms, particularly Tech giants Facebook, Amazon and Google are actively engaging with undergraduate students looking for talent with internships, co-ops and contract work during the semester. This is formidable competition because the tech giants have deeper pockets and fewer constraints then Federal agencies.

2. Education versus training

The critical shortage of cyber security workers has contributed to the rise of cyber security certification business. DODD 8140 (and its predecessor DODD 8570) ensures a government requirement that must be met. Additionally, non-defense industry also seems to favor graduates who have earned commercial cyber certifications such as Security+, CEH, CCNA-sec, etc.

Training, "the action of teaching a person or animal a particular skill or type of behavior" differs from education, "the process of receiving or giving systematic instruction." You can train someone to program in Ada and you can educate him/her in computer science to include programming skills. We train programmers in specific languages/environments and educate software engineers. Training is important, but tends to be of shorter-term value. Training strategies can

certainly be used as a stopgap measure to address critical personnel shortages. The Cybercorps program must remain focused on educating the cybersecurity workforce. Federal agencies may need to train new hires in specific skills Education is needed to provide the foundation for life long learning. Education on fundamental principals is the only way to "future proof" the education we can provide. Consider Coffman and Denning's 1973 classic *Operating Systems Theory*. It won't train a student on the Windows registry but the operating system design principles espoused in this work are still valid fifty years later.

3. New Technology and Cybersecurity education

University cyber security programs are challenged with having an increasing number of topics to cover. The NSA CAE Cyber Operations Program is an example of a specialized set of cyber security knowledge units that incorporate both current subjects as well as older fundamental subjects such as assembly language programming and reverse engineering as well as cyber operations tradecraft. The result is an academic program that is difficult to fit into a traditional degree program.

The NSA CAE-CO program is clearly geared to the production of cyber security scientists and engineers. While NSA is focused on the deeply technical side of cybersecurity, NSF CyberCorps meets a broader range of Federal government requirements including cyber security policy and information systems focused cyber security programs. An early lesson learned from the NSA CAE – CO effort is that it is very difficult to get deep coverage of all desirable cyber security skills in a single degree program. In NSA's case, there is also a need for its cyber security workforce to have specialized knowledge of intelligence tradecraft.

But the needs of the NSA are not necessarily representative of the entire Federal workforce. Different agencies have different cybersecurity workforce demands that are not all engineering based. Here is where the private sector needs differ from the public sector. Industry is demanding cybersecurity scientists and engineers and has much less demand for cyber policy and other "softer" cyber security skill sets.

New technologies are complicating this challenge. We are long way from having a single computer security course in a computer science program that was the norm fifteen years ago. Cyber security in software applications has expanded into other engineering disciplines and other colleges. Cyber security for SCADA systems, industrial control systems, IoT devices and High Performance Computing assets all require deep, specific technical knowledge that likely will lead to more and more specialized cyber security education and training programs. CyberCorps will receive applications from some of these newly formed, specialized programs and will need to consider whether these programs should become part of the SFS Scholarship program. This will further complicate the tradeoffs between technically and non-technically based CyberCorps educational programs. Should CyberCorps be cognizant that industry demands for cyber security professionals differs from government demands and plan accordingly?

4. Future Directions

ABET's recent move to accredit cybersecurity engineering academic programs is an important development. Future Cybercorps solicitations may wish to consider ABET accreditation in cybersecurity when evaluating new programs, particularly programs that do not fully meet the CAE criteria.

The author of "Dilbert," Scott Adams when asked, when asked if he had any advice for engineers, replied, "Engineers should work in organizations that value engineering." Having personally retired from Federal Service I doubted that government service would value engineers. However cyber technologies are rapidly changing that. NSA is clearly an organization that values engineers. Cyber technology is changing the Federal workspace and the security challenges are not only coming from amateurs and fraudsters, but also from nation state actors. While technology alone may not be sufficient to change attitudes in the Federal workspace, CyberCorps can and has. As more and more CyberCorps graduates rapidly advance

to leadership positions in the US Civil Service, they bring a new perspective to Federal cyber security that must continue to be nurtured.

Hamilton Bio-Sketch

Drew Hamilton is the Director of the Center for Cyber Innovation at Mississippi State University, a professor of computer science and engineering and leads the MSU NSF CyberCorps program. Previously he served as an Alumni Association Professor of Computer Science and Software Engineering at Auburn University where he initiated and led Auburn's SFS Program. He previously held faculty appointments at the US Military Academy and a visiting appointment at the US Naval Postgraduate School. Dr. Hamilton earned his doctorate in computer science from Texas A&M University. Dr. Hamilton is a distinguished graduate of the Naval War College