US scholarships aim to close cybersecurity gap

September 29 2012, by Rob Lever

Analysts at the National Cybersecurity & Communications Integration Center (NCCIC) in Arlington, Virginia, in 2010. Full tuition, expenses and a stipend will be paid by the US government at any of dozens of universities for students to get specialized cybersecurity training, in exchange for an equal number of years working for a federal agency.

For students seeking to become cyber warriors, the US government has a sweet deal.

Full tuition, expenses and a stipend will be paid at any of dozens of universities for students to get specialized cybersecurity training, in exchange for an equal number of years working for a federal agency.

The CyberCorps program launched in 2000 highlights how desperate the US government is to get people with the special skills to keep computer

networks secure.

Backers of the program say it is having a modest impact in meeting the country's growing cybersecurity needs.

"We have a large number of people who are students of cybersecurity, report writers, analysts," Alan Paller, research director at the SANS Institute and head of a task force advising the Department of Homeland Security on cyber skills.

"And we have a very small group who are the hunters. They are the ones who find out how the bad things happen and how to stop it."

Paller said there is intense competition for the small number of highly trained individuals.

"Every single company is searching for these hunters," he said.

Since the program was launched a decade ago, more than 2,000 students have received scholarships from the program, which is now available through 46 US universities.

Victor Piotrowski, program director for the CyberCorps, said the effort is aimed at boosting a "very small pool of people who have cybersecurity training."

The program funded through the National Science Foundation currently provides graduates around 150 students each year. But that is small compared with China which trains "a thousand times more" people, according to Piotrowski.

It is difficult to find people with science and technology background, but cybersecurity adds more requirements—those working for US

government agencies must be US citizens, without any criminal records.

Piotrowski said each year some 40 to 60 federal agencies compete for about 150 graduates, virtually ensuring a job for each.

"I can't think of any other profession which attracts so many agencies," he said.

Highlighting the shortage, Piotrowski said some graduates—who are required to work in government for the same number of years for which they receive a scholarship—sometimes get job offers from the private sector which allow them to bypass that requirement by paying back the government.

But Piotrowski said it's not necessarily bad if students move on to the private sector.

He said a large number of graduates go to top-secret jobs at places like the National Security Agency, but that all organizations need cybersecurity, from the Federal Reserve to utility companies.

"The argument is that defending cybersecurity is not only a government effort," he said. "We are only as strong as the weakest link. So by that reasoning it is not a loss."

The program offers aid similar to that of Reserve Officer Training Corps, which offers student aid for those going into the military.

Andreae Pohlman, a recent graduate of the program at George Washington University who is set to begin a government job, said the training included real-life attack and defense simulations which included some surprises.

In one competition, "We didn't know there were already back doors in our machines. We thought we were winning the whole time."

This offered a valuable lesson, she said: "It's important to get experience and exposure about the type of exploitation tools out there."

Mischel Kwon, another George Washington cybersecurity graduate who went on to head the US Computer Emergency Readiness Team before starting her own consulting firm, said awareness is a major issue.

"A lot of the problem is understanding we have a problem," she said.

"The workforce needs to grow and I think CyberCorps is a great way of doing that. We need to educate executives and company boards and help heads of agencies understand this is a priority that needs to be funded."

Patrick Kelly graduated from the GWU program and now teaches there in addition to his work at a federal agency.

Kelly said he tries to get students to learn about a range of possible threats like "phishing" e-mails, physical attacks and data thefts from portable thumb drives.

But he said the bad guys are constantly changing tactics.

"It's getting more severe," he said. "There is now an ability to automate attacks. The number of attacks and successful ones are going up exponentially, you're always playing catch-up."

Piotrowski said that the program has little trouble securing funding from Congress. In fact, he said lawmakers added $20 million to the $25 million requested a year ago.

"We don't have a problem defending the program," he said.

Paller said there is a growing concern that "the next war will be in cyberspace" and that the US is ill prepared.

We are pretty darn good at figuring out how to do attacks," he said. "But we are much more vulnerable to these attacks than everyone else."

(c) 2012 AFP