

Government, Military Face Severe Shortage Of Cybersecurity Experts

BY ERIC BEIDEL AND STEW MAGNUSON

"It takes a network to defeat a network," military leaders were fond of saying as they went after insurgents in Iraq. But there are other enemies out there who operate unseen and are attacking the United States. Cyberspies, hackers, and others using the Internet for nefarious purposes also operate in networks.

China, Iran and Russia host untold numbers of hackers. Whether they are state-sponsored or not is a matter of conjecture, but what is known is that they are relentless. U.S. military and civilian agencies are attempting to counter nonstop computer attacks and intrusions.

But do they have a network to counter them? There is an acute shortage of Internet security experts in the government, and no large pool of applicants waiting in the wings to join the fight.

"We need to be on the cutting edge with everyone else, from the teenager to the terrorist," Lt. Gen. Michael Basia, vice commander of Air Force Space Command, said at the Space Foundation's Cyber 1.1 conference in Colorado Springs, Colo., earlier this year. "For this domain, big brains are more important than big guns or big brawn."

Citing Department of Education statistics, Roger Cressey, a senior vice president at Booz Allen Hamilton, said U.S. universities bestow about 9,000 computer science degrees each year. Parks and recreation degrees come to about 25,000.

"I'm a big fan of Amy Poehler and the show Parks and Recreation, but if that is what is motivating our youth to go in that direction, then we have a challenge in front of us," Cressey said at the conference.

The government, weighed down by a ponderous hiring process, is having a difficult time bringing on personnel with expertise in network security, Cressey said.

Entities such as the Department of Homeland Security can hire firms such as his to supply contractors, but Booz Allen Hamilton is in the same dogfight to attract and retain talent.

There simply isn't a large number of cybersecurity experts — ones with extensive experience — currently collecting unemployment checks.

"It's pure supply and demand right now. The demand has never been higher, [and] the supply is limited, so a lot of firms like us, we're recruiting against each other," Cressey told National Defense. The long-term solution is to nurture the next generation of cybersecurity experts in high schools and universities. That will take time, and meanwhile, there are no easy answers, he said.

For the federal government, the problem is particularly acute since it has an infamously long, laborious hiring process, and most jobs require a security clearance.

DHS with great fanfare announced in 2009 that it would hire 1,000 cybersecurity experts. At a House Homeland Security Committee hearing, Philip R. Reiting, deputy undersecretary for the

National Protection and Programs Directorate, admitted that the department has fallen far short, and has only brought on some 260 new personnel. The new goal is 400 by October 2012. This comes at a time when the White House is giving more responsibility to DHS to protect computer networks in not only the civilian departments, but in the private sector as well.

Cressey said there is no escaping the fact that there will be a gap between now and the day when the next generation of cybersecurity experts comes up through the U.S. educational system.

"How do we bridge that?" he asked. "I think that is bedeviling and perplexing a variety of agencies in the government, right now."

Barbara Massa, vice president of global talent acquisition at internet security provider McAfee Inc., said cybersecurity experts with eight, 10 or 15 years of experience are scarce nowadays.

"There are only so many of them to go around," she said in an interview.

"It is a mistake for us to have such a shortsighted view and think we can only be trying to find talent from experienced people who are already in our industry. That's a recipe for failure," she said.

Bringing in information technology specialists from fields outside of computer security is one pool of potential recruits, as are former military personnel. They have great leadership and teamwork skills that may fit well in the organization. McAfee has training programs that bring these recruits up to speed on the world of cybersecurity.

However, the company's global threat intelligence team still requires "the best and brightest in the world. That is certainly not an area where we are looking to train," Massa said.

When it comes to competing with the government for talent, she suspects that with a work force of about 6,000, somebody has probably left McAfee to take a federal job. The company does not have that kind of data.

"There aren't any specific cases that I am personally aware of," she said.

The human resource department's philosophy is to make the hiring process as clear, speedy and as free of hoops to jump through as possible. It should mirror the way the company does business, she said.

Contrast that with the notoriously slow, opaque and bureaucratic federal hiring process where — even after a job offer is made — the candidate must go through a lengthy security clearance process that can take six months to a year.

Cressey said: "Our clearance process — to be kind — is constipated."

A recent survey by clearancejobs.com showed that the process is improving. Almost three-quarters of clearances are issued within 6 months, it said. Backlogs have fallen significantly during the past five years, it said.

A recent job posting on usajobs.gov for a position at DHS'



"We are always on the lookout for ways to improve the attraction and engagement during the hiring process from a candidate's perspective. The processes can't be overly bureaucratic and they can't be overly laborious," she said.

The hiring process is where McAfee makes a good first impression. There are many choices out there for these types of experts and the hiring process should reflect the company as a whole and show them that it is a great place to work, she said.

If a federal cybersecurity new hire has a security clearance in hand, he or she may be able to shorten the timeline. The problem is that there are different types of clearances and one that works at a certain agency might not be valid at another, Cressey noted.

The clearance system needs to be reformed, Cressey said.

Meanwhile, the gap in supply and demand is not going to go away, Cressey said. The nation can mitigate this in the future if it strengthens science, technology, mathematics and engineering education in U.S. public schools.

"It's a little bit of a zero sum game until you get that next talent pool trained and ready to go," he said.

Industry executives said cyberwarriors also need a more defined career path. Some experts believe that cybersecurity needs its own four-year curriculum, just like engineering or business administration. But defining the parameters of such a degree program won't fill the nation's immediate need for network defenders, and hiring professionals may be focusing their efforts on too safe a crowd.

"We're in a cyberwar today," Lynn Dugle, president of Raytheon's intelligence information systems businesses, said at the Air Force Association CyberFutures Conference in National Harbor, Md. Imagine if a general were informed that he would enter the battle tomorrow outmanned 10 to one, she said. "I don't think his response would be, 'Well, great. We're going to create a four-year college curriculum and we're going to fill the gap.'"

Recruiters have been looking in all the wrong places for fresh talent, Dugle said.

"We go to prestigious universities, we look for high performers, we have a minimal grade-point average and that's where we recruit talent," she said.

But none of Raytheon's recent and most impressive cybersecurity hires have come from the campus culture. One had only a GED and was working in a pharmaceutical plant stuffing pills into bottles. In the evenings, he outshined the rest during online hacker competitions.

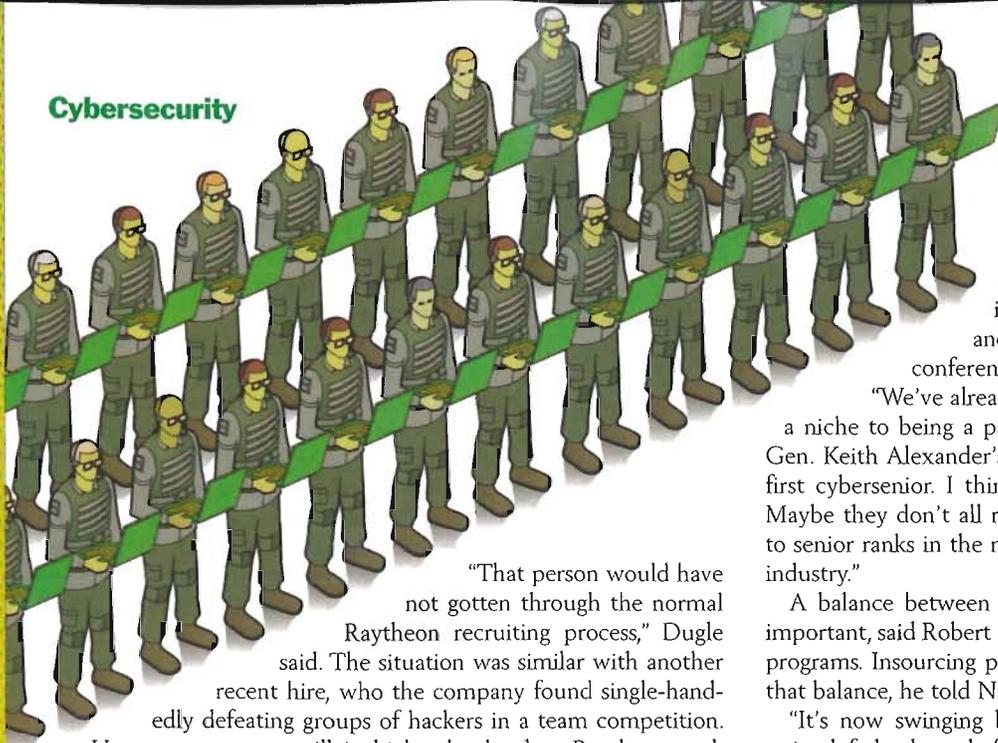
national cybersecurity division said applicants would have to wait four to six weeks for an answer as to whether they have made it through the initial screening. After an interview process that will last an undetermined length of time, they will have to wait to obtain a top-secret security clearance before starting the job.

DHS public affairs representatives did not respond to phone calls seeking comment.

Massa scoffed at a recruitment process that would take months. "If it even takes us two weeks to get an offer in a top talent's hand, that is too long," she said.

McAfee hires some network security specialists who have security clearances in hand to work on government contracts.

PHOTO-ILLUSTRATION BY BRIAN TAYLOR



“That person would have not gotten through the normal Raytheon recruiting process,” Dugle said. The situation was similar with another recent hire, who the company found single-handedly defeating groups of hackers in a team competition.

He was a teenager, still in high school, when Raytheon took notice. The company followed up and eventually made a job offer.

But the companies and agencies in dire need of network security professionals often lose out in the end. Corporate culture favors people who work nine to five, follow a dress code and are eager to move up the agency ranks. Computer savvy talents won’t be attracted to that environment the way they might be to a pay-for-performance scheme with less strings attached, Dugle said.

Steven Kenney, business director at Toffler Associates, said at the Cyber 1.1 conference that there can be a cultural conflict between the uptight world of military and civilian agencies and some of these nontraditional recruits.

“We hear the talk about wanting to put ethical hackers into our teams ... But are these the kinds of people we feel comfortable having in our organizations?”

Some of the best talent is not in the United States, he noted and he wondered if the nation can tap into overseas resources and trust those it recruits.

Dugle said: “What if we incentivized people by saying, ‘For every vulnerability that you find or every problem that you solve I will write you a check. I don’t care when you’re in the office or if you’re in the office.’”

Companies also have begun grooming their existing work force to defend their networks and the information they hold.

At Northrop Grumman, more than 1,000 employees this year will attend an internal Cyber Academy. All of the company’s employees need basic cybersecurity skills, Robert Brammer, chief technology officer for the firm’s information systems sector, said at the CyberFutures conference.

“Cybersecurity is not only about computer science and PCs and technical aspects like that, but it really is a much broader issue,” he said. Northrop Grumman requires that all of its employees know how to use the company’s access management system, protect their identities and recognize malware, phishing attempts and other threats.

The company has sponsored a CyberPatriot competition hosted by the Air Force Association, as well as hired the captain of last year’s winning team. But companies must show young talent that there is a path that takes advantage of their skills to advance, Brammer said. Northrop Grumman has promoted cybersecurity professionals into management positions, and though none has reached the level of sector president or corporate CEO, “I think that is

certainly possible.”

One day the Air Force will have a chief of staff who has worked his way up through the ranks as a cyber-expert, Barbara Fast, vice president of cyber and information solutions at Boeing Network and Space Systems, said at the CyberFutures conference.

“We’ve already seen where cyber has moved from being a niche to being a path to a senior role,” she said, citing Army Gen. Keith Alexander’s heading up Cyber Command. “He is the first cybersenior. I think there will be many other cyberseniors. Maybe they don’t all rise to the four-star level, but they will rise to senior ranks in the military and they will rise to senior ranks in industry.”

A balance between talent in the public and private sectors is important, said Robert Giesler, SAIC senior vice president for cyber programs. Insourcing practices over the past few years have upset that balance, he told National Defense.

“It’s now swinging back, recognizing that a healthy mix of a trained federal work force is critical but you’re never going to be able to solve the cyberproblem with just an insourced federal work force,” he said. “It’s got to be a very healthy dynamic balance between federal employees and contracting work force to address such a dynamic threat. I think we’re reaching equilibrium where a year ago, certainly two years ago, I would have been very pessimistic of where we were headed.”

But while the buzz has been all about hiring Internet warriors, the true defense system is already in place in the existing work force, from network security specialists to secretaries, Giesler said.

“The problem with cybersecurity right now is that the work force itself is the main target,” he said. “People have to know that they are the first point of attack on any successful network penetration.”

Companies that have had their networks breached were the victims of hackers who analyzed the staff, found specific individuals and sent them unique emails and URLs to click on, Giesler said. The only way to stop these kinds of intrusions is to educate employees, he added.

“You get the best return on the investment — not by buying additional hardware and technology for network security — but by actually spending a minuscule amount on training your work force,” he said.

Academic programs alone won’t attract the most promising talents to the field, Giesler cautioned. In the past 30 years, the most innovative cyber-operators he has seen have been military kids with no more than a high school education. “The talent isn’t necessarily academically derived,” he said. “It’s almost like linguistic skills that are inherited or that are naturally acquired. Because it really is a natural abstract language.”

“We’re almost at the point of deficiencies in the cybersecurity field,” Giesler said. “The country needs to understand that this is more than just hiring people. It needs to be infused all the way through the school system as a viable career choice, as something that everybody has to be familiar with, and we haven’t had that call to action yet.”

The cybersecurity movement needs a “JFK moment,” Giesler said, referring to the 35th president’s challenge to reach the moon by the end of the 1960s.

“It was visionary, it was a challenge and it was backed up by investment.”

ND

Email your comments to EBeidel@ndia.org or SMagnuson@ndia.org

ISTOCKPHOTO