MINORITY SUPPORT University consortium to boost diversity using NSF funds **p.519**

DISCRIMINATION Race found to be a barrier in the behavioural sciences **p.519**

NATUREJOBS For the latest career listings and advice **www.naturejobs.com**

MARK AIRS/IKON IMAGES/CORBIS

COMPUTER SCIENCE

Hacking into the cyberworld

Scientists are well placed to enter the growing, under-supplied cybersecurity workforce.

BY BRYN NELSON

In mid-November 2013, shadowy saboteurs attacked and crippled multiple sections of the electric grid in the United States. The previous day, assailants sponsored by a rogue government had struck at the heart of London's investment-banking industry, four months after a similarly brazen assault on New York's Wall Street firms.

Fortunately, the mayhem unleashed was only simulated. The three independently planned 'war games', respectively code-named GridEx II, Waking Shark II and Quantum Dawn 2, were designed by financial and government officials to test defences and responses to the growing threat of cyberattacks. GridEx II alone involved more than 1,800 participants from 200 government and utility organizations in the United States, Canada and Mexico, part of a major emergency drill aimed at improving the agencies' crisis action plans.

Why go to such lengths? The magnitude of the cybersecurity problem is massive. In the United States, President Barack Obama called it "one of the most serious economic and national security challenges we face as a nation". The threat is growing as crucial infrastructure — everything from energy and security to transportation and telecommunications — becomes increasingly reliant on the Internet.

"One thing is clear: the attacks are increasing in number, frequency, sophistication and damage," says Abdou Youssef, chairman of the computer-science department at George Washington University (GWU) in Washington DC.

Accompanying the growing risk is a huge demand for cybersecurity expertise, creating an unprecedented opportunity for physicists, computer scientists, mathematicians and other researchers with the right skills who are looking for a hands-on career option. Good candidates are finding jobs in government, academia and industry, says Jennifer Havermann, an engineering manager for international defence contractor Raytheon in Waltham, Massachusetts. From identifying vulnerabilities and designing firewalls to investigating security breaches, she says, the sector offers career paths that cater to backgrounds as varied as physics and behavioural psychology. "I think there's enough diversity in the field that there should be something for everyone," she says. "We need more of everything" (see 'Women and young people needed').

Irrespective of speciality, employers say that some traits are universally appreciated, such as an ability to analyse large data sets, think critically and see the big picture. Attention to detail, composure under pressure and a willingness and ability to adapt and continuously learn also help job candidates to stand out, says Youssef, who initially trained in maths at The Lebanese University in Beirut.

WIDESPREAD DEMAND

Cybersecurity essentially means defending a computer or group of computers from attempts to break into or hack a system or network and steal, change or destroy information. These cyberattacks originate from hard-to-trace sources and often consist of software known as viruses, worms, bots or Trojan horses, depending on how they infect, proliferate and inflict damage.

The cybersecurity field is frequently likened to chess, soccer or other games that reward a well-executed strategy and the ability to anticipate opponents' next moves. "I want to figure out how people can beat me — and stop it before it happens," says Markus Jakobsson, a cybersecurity expert in the San Francisco Bay Area and formerly the principal scientist at PayPal. The best cybersecurity professionals, he says, are curious, sneaky, smart and passionate about solving hard problems.

Around the world, multinational corporations such as Northrop Grumman and General Dynamics in the United States, BAE ▶

▶ Systems in the United Kingdom, Trend Micro in Japan and Thales Group in France are snapping up cybersecurity specialists. “Big companies are fighting for good security people,” says Jakobsson. “There are more open positions than there are available experts.”

RAPID EXPANSION

The same is true for the rapidly expanding roster of cybersecurity start-ups. When Michael Geppi founded Integrata Security in Baltimore, Maryland, in October 2012, he was the firm’s sole employee. Now there are eight, including several with master’s degrees in engineering. Geppi, the chief executive, hopes to add at least 20 more employees within the next 18 months.

He sees a huge demand for college graduates with degrees in engineering, computer science or maths. The extensive use of mathematical algorithms in detecting signals that might indicate criminal activity, and in designing security-minded computer software and hardware, also plays to the strengths of physicists, he says. “An advanced degree is not required,” he adds, “but with more tenure under your belt, it makes you very marketable” (see ‘Boot camps and degrees’).

Tasks vary. Some defence specialists try to outmanoeuvre criminals by developing antivirus software and other tools to prevent an attack. Penetration testers, or ethical hackers, instead play the part of attacker and try to breach a company’s computer network to identify weak points and recommend how to beef up security. Experts known as intrusion-detection specialists identify unusual patterns or signals that might point to a real cyber break-in. And some specialists develop codes to protect information or break codes to help identify and dismantle malicious software (malware).

ANTHONY RICHARDS

> **“An advanced degree is not required, but with more tenure under your belt, it makes you very marketable.”**
> Michael Geppi

Experts are also keeping a wary eye on attacks that allow criminals to breach wireless networks and infiltrate smartphones, tablets and other portable devices. But perhaps the biggest emerging danger is what the field calls an advanced persistent threat (APT). Instead of a lone hacker, well-funded groups sponsored by criminal organizations or governments often carry out these sophisticated attacks. “This is falling into the realm of cyberwarfare or cyberterrorism or cyber-organized crime, and that really ups the stakes,” says Marcus Rogers, head of the Cyber Forensics Program at Purdue University in West Lafayette, Indiana.

One recent high-profile incident illustrated the havoc that can be wrought by well-organized criminals. In December 2013, cybercriminals used malware to steal personal or financial information from an estimated 110 million customers of the Target store chain in the United States. The retailer has not disclosed many details of the data breach — one of the largest ever reported — or how it is now beefing up security. Experts say, however, that an effective response generally requires the services of forensic specialists, who can determine how the criminals gained access, how to contain the damage and how to prevent a repeat occurrence. Cybersecurity expert and blogger Brian Krebs in Annandale, Virginia has suggested that a “malware-laced” phishing e-mail sent to employees of an independent Target contractor might have allowed criminals to swipe credit-card data from cash registers in retail stores. By scrutinizing this type of malware, investigators might be able to determine how it infected the computer system and where it originated.

CYBERSCIENTIST

Rogers, who trained as a forensic psychologist and once worked as a detective, says that it can be “surprisingly easy” for scientists to make the transition to cybersecurity, even if they do not have a strong background in computer science. “A strong foundation in science itself — the scientific method, hypothesis testing — and even a rudimentary amount of statistics allows you to transition to this area very quickly,” he says. “The technology area of what we’re dealing with isn’t really the hard part. It’s trying to figure out what’s coming next.”

At Purdue University, students can obtain PhDs in interdisciplinary information security from the university’s Center for Education and Research in Information Assurance and Security — and the centre boasts a 100% placement rate for its graduates, Rogers says. The roughly ten students enrolled at any given time come with backgrounds ranging from criminology and psychology to physics and maths, and pursue projects sponsored by a dozen academic departments. “Most of the students are offered two or three different jobs and internships,” Rogers says. Potential employers, he adds, are “almost getting into bidding wars”.

Graduate students who are pursuing other degrees can take cybersecurity classes on the side to explore the potential security applications of their research. During his PhD coursework in computer science at GWU, Moroccan native Anasse Bari also completed a graduate certificate programme in Computer Security and Information Assurance, a common academic discipline in the cybersecurity field. His classes, including one on computer security and another on information policy, helped him to realize that his research on a data-mining algorithm — inspired by flocking birds and called Flock by Leader — had a strong security tie-in.

Now a visiting assistant professor of computer science at GWU, Bari uses the physics of how birds fly in formation to detect ‘flocking’

UNTAPPED POTENTIAL

Women and young people needed

Cybersecurity may be a growing field — but not everyone is aware of the job potential. A 2013 survey commissioned by international aerospace and defence contractor Raytheon in Waltham, Massachusetts, revealed a lag in enthusiasm for the field among 18- to 26-year-olds in the United States. Fewer than one in four said they were interested in a career as a cybersecurity professional, near the bottom of 14 options ranging from an entertainer (the most popular) to a Wall Street analyst (the least popular). The results also highlighted the field’s significant gender gap: 35% of young men but only 14% of young women showed an interest in the career.

Lisa Foreman, a freelance information-security consultant based in the Washington DC area, founded the Women’s Society of Cyberjutsu in 2012 to encourage more girls and women to consider the career choice. “I wanted to create a community where women can come together and learn in a comfortable learning environment,” she says, “and have a place to go and really geek out without feeling intimidated.”

The society sponsors monthly workshops that offer hands-on experience for women who want to learn more about particular cybersecurity tools or topics such as web app security, digital forensics and ethical hacking. It also fields teams in fast-paced ‘capture the flag’ challenges that test participants’ cybersecurity skills by requiring them to defend their own systems from an attack while trying to hack into those of other teams. The Women’s Security Society has a similar role in encouraging the advancement of women in the profession in the United Kingdom.

“I think it’s especially important that women who are in the career field share their stories,” says Jennifer Havermann, an engineering manager at Raytheon. During a trip in October 2013 to talk to students at a cybersecurity fair hosted by California State Polytechnic University in Pomona, she was inundated by questions about the field and her own career trajectory. “I’m really encouraged,” she says. **B.N.**

E-SKILLS

Boot camps and degrees

For job applicants with the right core skills, companies and government agencies often provide the training for specialized tasks. But how can job seekers acquire the skills that will get them noticed?

Among degree-granting cybersecurity institutions, Carnegie Mellon University's CyLab in Pittsburgh, Pennsylvania, the Lincoln Laboratory at the Massachusetts Institute of Technology in Lexington and the Maryland Cybersecurity Center at the University of Maryland in College Park are some of the best-known US programmes. In the United Kingdom, the University of Oxford and Royal Holloway, University of London received £7.5 million (US$12.5 million) in government and research-council funding in 2013 to offer multidisciplinary PhD degrees in support of national cybersecurity interests.

Beyond a degree, most job seekers must also earn some form of professional certification. One of the field's most important is the CISSP (Certified Information Systems Security Professional), which is commonly required for government work. Another is the CEH (Certified Ethical Hacker), which applies to professionals who help clients to bolster their defences through simulated attacks, or penetration testing.

Institutions often provide certification training for their own workers or students. Other individuals can study at university-sponsored or corporate training centres that host intensive one-week boot camps costing US$2,000 to $4,600 or more. With names such as Intense School and SecureNinja, these programmes run students through a rigorous regimen of drills and reviews to prepare for the certification's final examination. B.N.

patterns that can be applied to groupings of similar people, tweets, Facebook data, documents and other information. As a security tool, the work might help to identify leaders and followers in online communities and use that knowledge to predict criminal activity or to detect fraud.

A strong background in maths, meanwhile, might provide an advantage for cryptography, a subspeciality that involves writing or breaking secret codes that are designed to protect data or channels of communication. Peter Ryan, professor of applied security at the University of Luxembourg, had been fascinated by codes since childhood, but began exploring cybersecurity only after receiving his PhD in mathematical physics from the University of London. He later found a job in cryptography at the UK intelligence agency Government Communications Headquarters.

At the University of Luxembourg, Ryan uses some of the same maths-based methods to make touch-screen and other electronic voting systems less vulnerable to tampering. "We try to imagine how an attacker might attack these and, as best we can, develop techniques to foil all of the attacks we can come up with," he says.

Other specialists have found a niche in quickly neutralizing potential cybersecurity threats. Krysta Cox, an analyst for ManTech International Corporation based in Washington DC, describes her job as an emergency medical technician for computer networks — "you're the first responder when an incident happens", she says. If an employee at one of her corporate clients receives a suspicious e-mail that asks the reader to follow a link and reset a password, Cox sequesters the message within a secure system that is isolated from the rest of the computer network. Then she clicks on the link to see where it leads. If the destination spells trouble, she can capture the information and instruct the computer network to automatically flag similar e-mails to prevent future risks.

Anyone wanting to enter the cybersecurity job market should be aware that irrespective of speciality, stringent background checks are routine, especially for a government agency or a private contractor working closely with one. "You need to expect investigators to go over every single aspect of your life," says Integrata's Geppi. Ill-advised Facebook posts, tweets and other social-media messages can come back to haunt potential job applicants.

And in many countries, positions within government or with government contractors may require proof of citizenship or long-term residency. Foreign students may have more success pursuing a job in academia, or with multinational companies.

Beyond these caveats, experts say that motivated individuals with strong scientific skills should be well positioned for a successful cybersecurity career. "Security is always a cat-and-mouse kind of game, and often the attackers are a bit ahead," Ryan says. "In a way, it's slightly depressing that it's like that, but in another sense it's actually quite fun. And it means that there's probably not going to be any shortage of jobs for people for a long time to come." ■

Bryn Nelson *is a freelance writer based in Seattle, Washington.*

EQUAL OPPORTUNITIES

Minority support

A consortium of four US universities aims to boost diversity in maths, engineering and physical and computer sciences with the help of a US$2.2 million grant from the US National Science Foundation. The California Alliance for Graduate Education and the Professoriate is being led by the University of California (UC), Berkeley, and includes UC Los Angeles, the California Institute of Technology in Pasadena and Stanford University. The universities aim to create a community of minority PhD students, postdocs and faculty members by providing training and funding travel between institutions. "We want to create an environment that's more welcoming," says Mark Richards, executive dean of the College of Letters and Science at UC Berkeley.

FELLOWSHIPS

Canada needs managers

The Canadian federal government is investing Can$8 million (US$7.3 million) over two years to tackle the country's shortage of research and development managers. Mitacs, a nonprofit organization in Vancouver, will run a fellowship programme to support 125 to 150 postdocs in industrial research, providing training in skills such as management and leadership. Researchers who have received a PhD from a Canadian university within the past five years can join the scheme. The employment rate is high for those who have finished the pilot programme, says Arvind Gupta, Mitacs chief executive and scientific director. "Researchers come out of the programme with the skills to manage a company's research portfolio," he says.

DISCRIMINATION

Race obstacle

One-fifth of workplace barriers faced by minority researchers in behavioural science are related to race, a study says (R. R. Kameny *et al. J. Career Dev.* **41,** 43–61; 2014). In addition to barriers such as a lack of mentors, early- to mid-career US minority researchers identified race-related hurdles such as colleagues' low expectations of performance and a lack of support for studies on minority groups. Minority researchers must seek help from faculty members who are capable of changing the department culture, says co-author Rebecca Kameny, a psychologist at the research company 3C Institute in Cary, North Carolina.