Of Mice AND a Menace

BY DANNY FREEDMAN

The tug-of-war for digital dominance requires an increasingly skilled crop of defenders. Enter GW CyberCorps.

When Homeland Security Secretary Janet Napolitano was asked at a forum last fall about the single thing she would do immediately, if she could do anything, to better secure cyberspace, the answer was blunt.

"I would have every cybergeek in the United States who's any good at detecting hackers and intrusions come work for me," she said at the *Washington Post* event, co-sponsored by GW's Cyber Security Policy and Research Institute.

Asked how many serious cybercrimes had probably occurred nationwide during her 45 minutes or so on stage, she ventured: "Oh, thousands. Thousands. Untold."

Around Washington, especially as Congress debated cybersecurity legislation this spring, warning calls have been pointing out a hidden and growing fire, like an urgent chorus of whistling kettles.

Cyberattacks "are increasing in frequency, in complexity, and in consequence," said Secretary Napolitano. They are mentioned in terms of national security: FBI Director Robert Mueller has said cybercrime is poised to overtake terrorism as public enemy No. 1; and in assessing readiness, parallels are being drawn to September 11.

Cybercrime, just like old-fashioned crime, runs the gamut from petty thievery and organized crime to espionage and the work of so-called hacktivists. Identities, money, intellectual property, state secrets, and public safety are on the line.

At the individual level, it's maybe even getting hard not to reluctantly shrug in the face of alarming statistics that make victimhood—or at least exposure to it—seem likely, if not inevitable.

Businesses could be in the same boat. "There are only two types of companies," Mr. Mueller has said. "Those that have been hacked, and those that will be."

And the government has its own problems. In April, federal auditors said the number of cybersecurity incidents and incidents under investigation that were reported by federal agencies jumped nearly 680 percent between fiscal years 2006 and 2011, from 5,503 to 42,887.

ILLUSTRATION BY DANIEL BEJAR

"Nearly 200": The number, in 2011, of known attempted or successful cyberattacks on the systems behind critical infrastructure facilities, like power plants, refineries, and transportation systems, according to an April *Washington Post* op-ed by John O. Brennan, President Obama's senior adviser on counterterrorism and homeland security. That's almost five times more than in 2010, he wrote.

Some of that is due to better detection and reporting, though the jump is still worrisome.

But the thing that has experts and officials wringing their hands is the thing we haven't encountered yet—a devastating shutdown of critical infrastructure, like the power grid, water treatment plants, the financial system, and nuclear facilities.

"We've come close in some instances," Secretary Napolitano acknowledged at the event.

Former National Security Director Mike McConnell, writing earlier this year in a *Washington Post* op-ed, didn't mince words: "The United States is fighting a cyber-war today, and we are losing. It's that simple."

To help turn the tide, GW's Cyber Security Policy and Research Institute is training and supplying the government with a small army of multidisciplinary, next-generation "cybergeeks."

Over the past decade the institute has been awarded nearly $10 million in federal scholarship-for-service grants for the more than 60 graduates of a program called the GW CyberCorps. Undergrads and graduate students receive full tuition plus a stipend—either jointly from the National Science Foundation and the Department of Homeland Security, or from the Defense Department—in exchange for an equal number of years of government service.

And they are being snapped up as fast as they're churned out; bidding wars have ensued.

"How many geeks did you want?" a man asked Secretary Napolitano at the event last fall.

"How many ya got?"

At its core, cybersecurity is a technical problem. But it's going to take far more than technical sharpshooters to find workable fixes, experts say.

"If you have [only] a technological solution, I can show you plenty of things that were great technology that didn't get adopted for one or another reason," says Lance Hoffman, director of the Cyber Security Policy and Research Institute, who runs the GW CyberCorps program and is principal investigator on the grants.

"You need people who know enough about the technology, and they know enough about policy, and governance," he says, "that they can put all three together to come out with a reasonable solution."

That goes equally for securing one system on a network, or designing a treaty for scores of nations.

So Dr. Hoffman and CyberCorps co-principal investigator Shelly Heller, a computer science professor and the Mount Vernon Campus' associate provost for academic affairs, have geared the program to train students in the mold of Washington: They are primed for offense and defense but also diplomacy and policy.

For starters, the students don't always hail from the usual academic silos. Many do come from computer science and computer engineering, but there also are students of public policy, forensic science, law, international affairs, and business.

Among GW's grant applicants for next fall, more came from the School of Business than anywhere else on campus, Dr. Hoffman says.

The common thread between them is a course called Information Security in Government, which GW CyberCorps students take each semester. In it students wade through the same issues facing the federal government.

One semester they focused on implementation of the Federal Information Management Security Act, for instance. And this past spring they studied the continuous monitoring systems that agencies are building to constantly screen for vulnerabilities in their systems.

The course covers how policies are created and the technical skills needed to implement them. In short, says Mischel Kwon, who leads the course: "I'm teaching them how to be government employees."

For the task, Ms. Kwon draws upon her own deep experience and the Rolodex of guest speakers that comes with it.

She is a product of the GW CyberCorps program, having received a GW certificate in computer security and information assurance in 2005 as a student at Marymount University, under a previous partnership with GW. She went on to top-level information security jobs at the Justice Department and to lead the U.S. Computer Emergency Readiness Team before starting her own information security consulting firm, Mischel Kwon & Associates.

In her CyberCorps course, Ms. Kwon leads a varied group of students across an equally diverse academic landscape. As a result, nobody stays in their wheelhouse for long.

"I like to say, [by the] fourth week in I have a cranky group of people," she says. "Those people that are computer science and technical, I'm pushing them to work with policy. Those that are more policy- and business-oriented, I'm pushing them to be technical. Then there are those people in forensics."

"I'm handing them a whole new ball of wax," she says.

It's a tough road, but one that affords students a certain luster with employers.

"The agencies do fight over them," Ms. Kwon says. "They know that they are just so capable right out of the box. And that's hard to find in the government—right away you've got a person that understands all the lingo, and the processes, and can fit right in and start working. That's unusual."

Others are noticing, too: Last year the National Science Foundation awarded Dr. Hoffman's institute a grant to essentially bottle and ship the course, through videos and instructor guides, to similar programs at the University of Hawaii and University of Washington. The idea is for the trio to share teaching tools and, ultimately, to create a library that would be available to CyberCorps-type programs nationwide.

"There's no shortage of problems to be solved in this space," says Joseph Mathews, BS '02, MS '04, one of the 64 students who have completed the GW CyberCorps program to date.

Since graduating, Mr. Mathews has been working as a computer engineer in network defense research at the U.S. Naval Research Laboratory in Washington. A security issue with any of the Navy's networks—covering land, sea, and sub, and comprising nearly a million computers, he says—might cross his desk.

Patrick Kelly, MPP '08, went to the Federal Reserve Board as an IT analyst and now works as a privacy official and branch chief in the Office of the Inspector General at the U.S. Department of Health and Human Services.

On paper, he has a decidedly nontechnical pedigree: undergraduate degrees in political science and philosophy, and a master's in public policy. But underneath it all is "a geek since birth," he says. There were computer classes as a kid, computer sales and web-design consulting by high school, a job in tech support during college. With interests in policy and computers he knew he wanted to end up in the federal sphere; he just hadn't known cybersecurity was an option until arriving at GW.

"On high school career day," he says, "they didn't tell me I could take computer classes on business intelligence and cyberwarfare."

Steven Moxley was weighing four job offers from federal agencies ahead of graduation this May, when he received a master's in international science and technology policy from the Elliott School of International Affairs. He chose the Federal Reserve, where he'll be primarily doing network defense work.

The program was "very helpful in actually showing me what the options are, and getting me in touch with the agencies that really do what I was looking to do," he says. "Otherwise, I don't really know how I would've gotten a foot in the door."

The clock struck 11 a.m. and, just as planned, the group gained access to the network.

At the front of the room, Andreae Pohlman stood between two projector screens displaying a list of freshly created passwords and, with a bit of urgency, told the assembled cybersecurity team: "Change your passwords right away. *Change, change, change*."

The network they were handed was likely riddled with holes, chief among them compromised passwords. Team

WILLIAM ATKINS

Andreae Pohlman, at the time a student in the business school and the CyberCorps program, helps lead GW's team in the National Collegiate Cyber Defense Competition.

members began hunting for other vulnerabilities and braced for an attack.

To the uninitiated, though, the room seemed more Internet café than command center.

Ms. Pohlman, at the time a graduate student, was in black Converse sneakers and a black T-shirt that read: "I am an advanced persistent threat," a little cybersecurity pun.

She and the 10 other students in the room, each at a separate computer, coordinated their defense duties over the static of clicking keyboards and mice. Adele's song "Rolling in the Deep" was playing. The smell of pizza wafted through the air.

The group was squaring off in the first round of the National Collegiate Cyber Defense Competition from a computer lab in Foggy Bottom. Four teammates, including co-captain Ms. Pohlman, were members of the GW CyberCorps.

The competition isn't mandatory for them, but Ms. Pohlman—who was preparing to start a new job at the Defense Information Systems Agency—says it helped bridge her business degree and her CyberCorps training.

In May, she completed a combined bachelor's in business administration and master's in information systems technology. While the degree work prepared her for managing an IT environment, she says, CyberCorps and the competition helped her "feel confident in knowing what sorts of threats are out there."

On this Friday morning in February, the team was protecting the network of a single, fictional medical practice. And things were going remarkably well as the competition neared the halfway mark.

A celebratory can of Silly String even made a premature cameo, before the owner reluctantly tucked it away again.

"Andreae, do we have control over all of our boxes? We haven't lost anything yet?" asked Mr. Moxley, then a graduate student as well, who co-led the team with Ms. Pohlman.

"Nothing yet," she said. "That's a good sign."

And a half hour later the status still hadn't changed. "We're almost in cruise control," she said.

When the evaluations rolled in, they found out why: The team members did such a good job battening down the hatches, they'd unwittingly cut off communication with the judges. Systems that the team knew were up and running appeared, from the outside, to be not even there.

"It just boils down to: I guess we were too secure," Ms. Pohlman says later in a coffee shop on campus, reflecting on the results.

The judges' inability to access the services on the medical practice's website torpedoed the team, despite an otherwise remarkable showing. In the other scoring categories, says Ms. Pohlman, the team was at or near the top of the heap.

It was a head-slapper of a loss. But it touched on the very heartbeat of the Internet and the great conundrum of securing it. The Internet only works—that is, it's only informative and useful and fun—when the fortifications still offer some way in; when there's a certain amount of insecurity.

Just how much insecurity is a question that every entity on the Web is wrestling with, right down to the protectors of a fictional medical practice.

"That's the billion-dollar question," Ms. Pohlman says.

The focus on computer security at the university reaches back more than three decades, and starts with Dr. Hoffman of the Cyber Security Policy and Research Institute.

"There's always been data to protect," he says, even if it was a time of "big computer rooms with computers you could actually walk through."

Dr. Hoffman arrived at GW in 1977 to launch its computer security offerings, seven years after he did the same at the University of California, Berkeley, where he started what he believes to be the nation's first regularly scheduled course on computer security at a four-year university.

"The same problems were still around, [now] they're just magnified in scale," Dr. Hoffman says. "Now they're global."

As one measure of that, GW recently announced a university-wide cybersecurity initiative (see sidebar) to link new and existing efforts across campus, from the schools of law to engineering to business.

Dr. Hoffman's institute, part of the School of Engineering and Applied Science, will be a piece of that initiative and provides successes for it to stand on: The institute led the effort to have GW designated a National Center of Academic Excellence in both information assurance education and research. The accreditation by the National Security Agency and the Department of Homeland Security makes the university eligible to compete for the federal scholarship-for-service grants.

The institute also has more than a dozen researchers affiliated with it, who dig into issues from cybersecurity to privacy, e-commerce, intellectual property, and education. Researchers also are exploring whether recipients of federal scholarship-for-service grants are inclined to stay with the government after their commitment is met, or jump ship.

Filling and retaining the cyberranks is as much an issue for the government as for businesses, says Shelly Heller, the co-principal investigator of the CyberCorps program. The need, she says, is "enormous."

As life became digitized, the demand for cybersecurity ballooned, says Dr. Heller, but the supply of cybersecurity professionals, which she characterized as "a trickle," has all but stayed the same.

"The government is in a situation, as is private industry, [where] there aren't enough trained, educated, focused professionals in the field," she says.

And the nation is flush with pressing issues for them to sort out: How can sturdy yet porous walls for the Internet be built? How, and to what extent, should government and industry work together to play defense? And what are the rules for offense?

"You basically have the problem of trying to keep the airplane flying while reinventing it at the same time," Dr. Hoffman says.

Fortunately, he knows several dozen good folks, with more on the way. GW

CONFRONTING THE Cyber Conundrum

The work of teaching, interpreting, and pushing at the front lines of cybersecurity is happening around the university. And this summer, a new initiative was announced to coordinate and bolster those efforts.

GW experts are in the classroom, in the lab, and being called upon to inform decision-makers and the public discourse.

"Cyber basically levels the playing field," Frank Cilluffo, director of GW's Homeland Security Policy Institute, said in April as he testified at a congressional hearing on the cyber threat posed by Iran.

Even small groups can make a big impact, he said, by simply renting or buying whatever capabilities they lack. "There's a cyberarms bazaar on the Internet. Intent and cash can take you a long way."

HSPI's leaders have become media go-to guys for security insight. And the institute has served as a node of policy analysis through its research and events, both closed-door and public—like the launch in May of the Capstone Series on Cyber Strategy, which featured former Vice Chairman of the Joint Chiefs of Staff Gen. James Cartwright.

Elsewhere around the university, among the work of many others in this realm: Diana Burley, in the Graduate School of Education and Human Development, is studying cybersecurity education and workforce development; Hoeteck Wee, in the School of Engineering and Applied Science, is designing cryptographic methods to stymie new types of cyberattacks; and Daniel Solove, at the School of Law, is mining topics in information privacy law.

The new university-wide cybersecurity initiative, formally announced in June by Board of Trustees member J. Richard Knop, JD '69, will link new programs with existing efforts, aiming to help illuminate issues at the core. Mr. Knop will chair the initiative's external advisory board, while Provost Steven Lerman and Vice President for Research Leo Chalupa will co-chair an internal advisory board.

"There's a real need for this that hasn't been filled," said Dr. Chalupa. "We want to be the go-to place not just in the region, but in the nation. When people want to know about the big questions in cyber finance, policy, and law, they'll come here. And the academic programs are going to buttress the whole thing in a big way."

The initiative launched with several elements already under its umbrella, including both longtime programs and new enterprises:

Master of Science in Cybersecurity in Computer Science: The new degree offered by the School of Engineering and Applied Science will be the first of its kind in D.C. Students will be trained to approach cybersecurity from a systems management mindset and will be able to make use of cybersecurity-related courses across GW.

Cyber Center for National and Economic Security: A new multidisciplinary policy center led jointly by Frank Cilluffo, of GW's Homeland Security Policy Institute, and Doug Guthrie, dean of the School of Business. Through research and events the center explores the challenges for businesses as cybersecurity policy is forged, which could mean trade-offs between competitiveness and security.

World Executive Master of Business Administration in Cybersecurity: This new degree, developed by the School of Business and HSPI, is aimed at both public and private sector professionals who work in areas that range from policy and contracting, to privacy and data security. There also are plans to offer customized programs for corporate clients.

Master of Laws in National Security Law: The degree is currently offered by the Law School and plans are underway to create within it a specialization in cybersecurity. Along with existing cybersecurity-related courses, such as "Law in Cyberspace," the Law School plans to develop courses that address the confluence of cybersecurity and government contracts, historically one of the school's strengths.

Doctor of Education in Human and Organizational Learning: A new cybersecurity-focused track is being added to the well-established, nearly 25-year-old degree from the Graduate School of Education and Human Development. The courses—held one weekend per month—will provide technical professionals with the training in organizational leadership, research, and analysis needed to manage people and security-conscious organizations.

Master of Professional Studies in Security and Safety Leadership: Offered by the College of Professional Studies and the GW Center for Excellence in Public Leadership, the degree is aimed at homeland security and safety professionals in the public and private sectors, and is offered in the classroom or online. Students can focus either in fundamentals of strategic security or strategic cybersecurity enforcement.

Cyber Security Policy and Research Institute: The institute runs the federal scholarship-for-service GW CyberCorps program (see article), facilitates research across the spectrum of cyber issues, and plays a leadership role in CyberWatch, a network of two- and four-year institutions working to boost the quantity and quality of the cybersecurity workforce.

ILLUSTRATION BY DANIEL BEJAR