A NEW FRONTIER FOR CYBERSECURITY

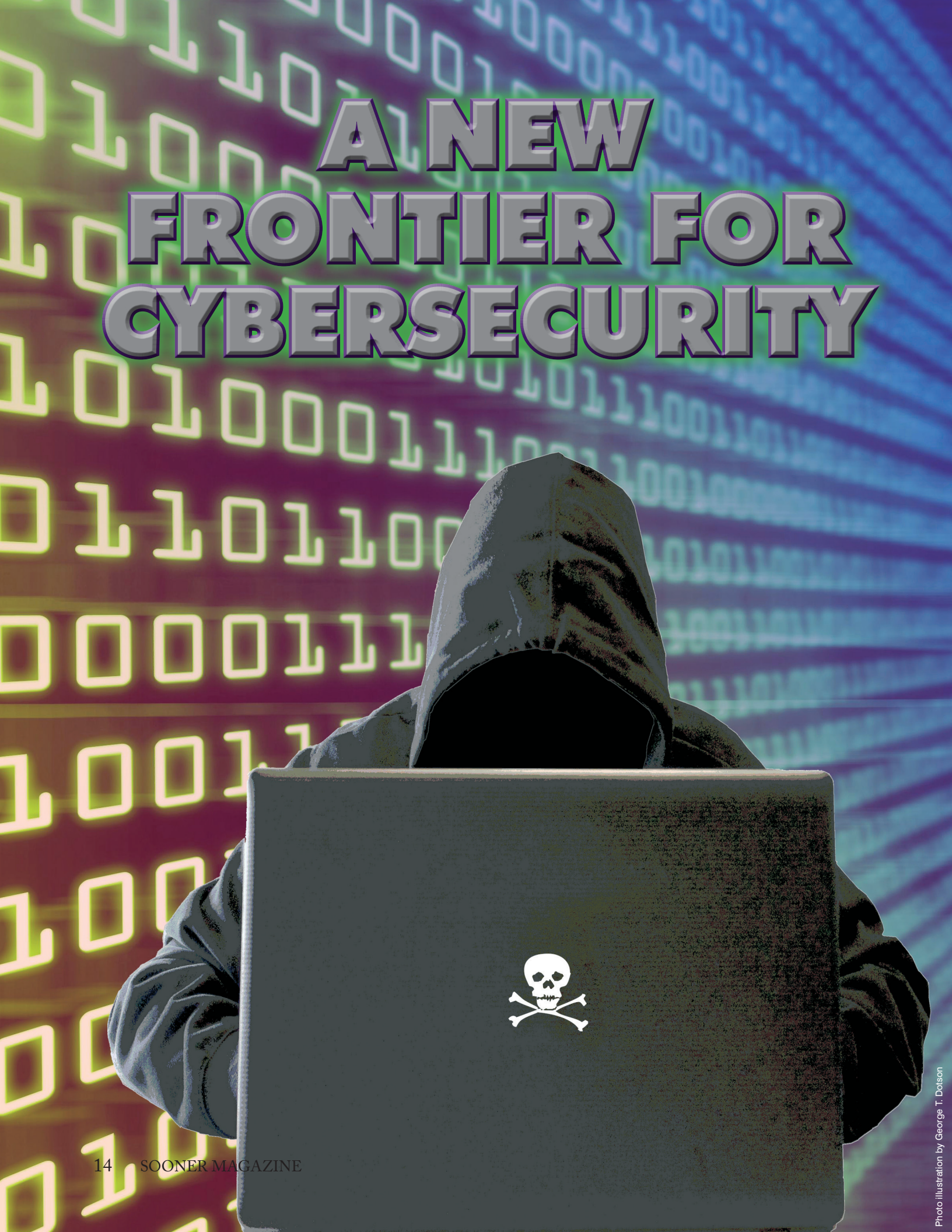

Photo illustration by George T. Dotson

Hacking victims from Sony to the DNC have left corporations and governments looking to the next generation for help.

By Tom Kertscher

Russian hacking that rocked the 2016 presidential campaign during its final weeks should have made it plain that, online, almost everyone is vulnerable.

"Governmental organizations have motivation to conduct political hacking," says Qi Cheng, the Williams Company Foundation Presidential Professor in computer science at the University of Oklahoma. "There are many foreign governments interested in influencing U.S. elections, just like the U.S. government has interests in other countries' political affairs."

In March 2016, Russian hackers sent a "phishing" email to the personal Google account of John Podesta, Hillary Clinton's campaign chairman. Phishing emails aim to get the recipient to click on a deceptive link that gives hackers access to their information.

Podesta correctly perceived that the email might be a hoax and sought advice from other campaign staffers. In response, one campaign staffer meant to tell Podesta that the email was illegitimate, but wrote legitimate - prompting Podesta to change his password.

Instantly, 60,000 of his emails were accessed by the hackers. Then in October 2016, as election day drew near, WikiLeaks began releasing the emails, which were used in attacks on Clinton.

The episode illustrates how one wrong move online can be devastating.

"I will certainly introduce the example in future courses," Cheng says. "I will ask students to read materials on the breaches and do presentations in class. But the students will have to look beyond news articles and read more technical details from professional magazines, research journals and conference proceedings."

Cheng received his Ph.D. in computer science from the University of Southern California in 2001 and joined the OU faculty later that year. His research interests include theoretical computer science, DNA/molecular computing, cryptography and computational number theory. He has published more than 30 research articles in journals and conference proceedings.

Cheng teaches two courses relating to security: Cryptography and Computer Security. Cryptography involves encryption and cryptanalysis. Encryption helps to protect computer users' privacy, while cryptanalysis will break weak encryption. Cheng describes it as similar to computer forensics and work that is done by the FBI and the CIA. Computer security involves how to use cryptography in practice to secure computer systems.

"I guess the classes are popular," Cheng says. "Sometimes they have long waiting lists."

The waiting lists are likely to grow with the demand for increased cybersecurity among U.S. government agencies, political organizations and private companies.

"Government has in-house security experts and they are more aware of hacking," Cheng says. "In fact, historically only government experts studied cryptography at the professional level. Government also classifies the data into different security levels, and applies strict access control policy on data of high, secure level. Even the communication channels between different agencies are encrypted."

Still, even if citizens can have confidence that sensitive government data is being protected, risks remain. Hacks of Yahoo, revealed by the company in late 2016, involved 1 billion user accounts in 2013 and 500 million in 2014. The two attacks are the largest known security breaches of one company's computer network, according to *The New York Times*.

"If one follows all the security procedures carefully, computer systems should be secure. But it is hard to do that," Cheng says. "Even if 99 percent of computers and servers are safe, the remaining 1 percent will create a lot of problems, and get into the headlines." Cheng says computer users shouldn't despair, however.

"Having common sense to deal with emails can prevent many problems," he says.

"Even if 99 percent of computers and servers are safe, the remaining 1 percent will create a lot of problems, and get into the headlines."

Cheng's tips for staying safe online include: Visiting only secure websites (with https) if personal information is involved; turning on the encryption option when using cloud data storages; and updating your computer operating system and applications often to reduce vulnerability.

Meanwhile, OU is beefing up its cybersecurity offerings.

"We are working on making a cybersecurity course as a required course in our curriculum," says Sridhar Radhakrishnan, director of the School of Computer Science. "Cybersecurity starts with writing secure code. We want our students to learn the art of writing secure code."

Tom Kertscher is a PolitiFact Wisconsin *reporter for the* Milwaukee Journal Sentinel. *He began his career at the* Tulsa World.