In the Trenches of CYBER WARFARE

By June L. Kim, Associate Editor

THE most dangerous threat to the United States may no longer come from a physical attack, but a cyber one. Terrorist organizations, criminal masterminds, enemy nation-states, and lone anarchists alike could cripple the United States if they gain access to networks that control power grids, gas and oil pipelines, transportation, banking, and financial systems. They could cause blackouts, flood towns, collapse the US economy, reroute gas and oil away from towns, and plenty more. So said James V. Christy II, until recently the director of futures exploration at the Defense Cyber Crime Center.

America's critical infrastructure is automated and controlled by supervisory controller and data acquisition, or SCADA, systems. Each SCADA system is a centralized computer that monitors, gathers, and processes data and determines what to do next. "It's not done by a little guy sitting in a room," said Christy during a November interview.

Imagine the Internet as the highway system, he said. The highway can lead anywhere and there are on-ramps and off-ramps that lead to smaller roads, or networks, that lead to homes, or different infrastructures. The SCADA system would be like the security system for one's home, he said.

"If you can get past the lock on the door, you can break into anybody's house," said Christy, and with the Internet "the highway system got you there. … You could break into the system from anywhere in the world."

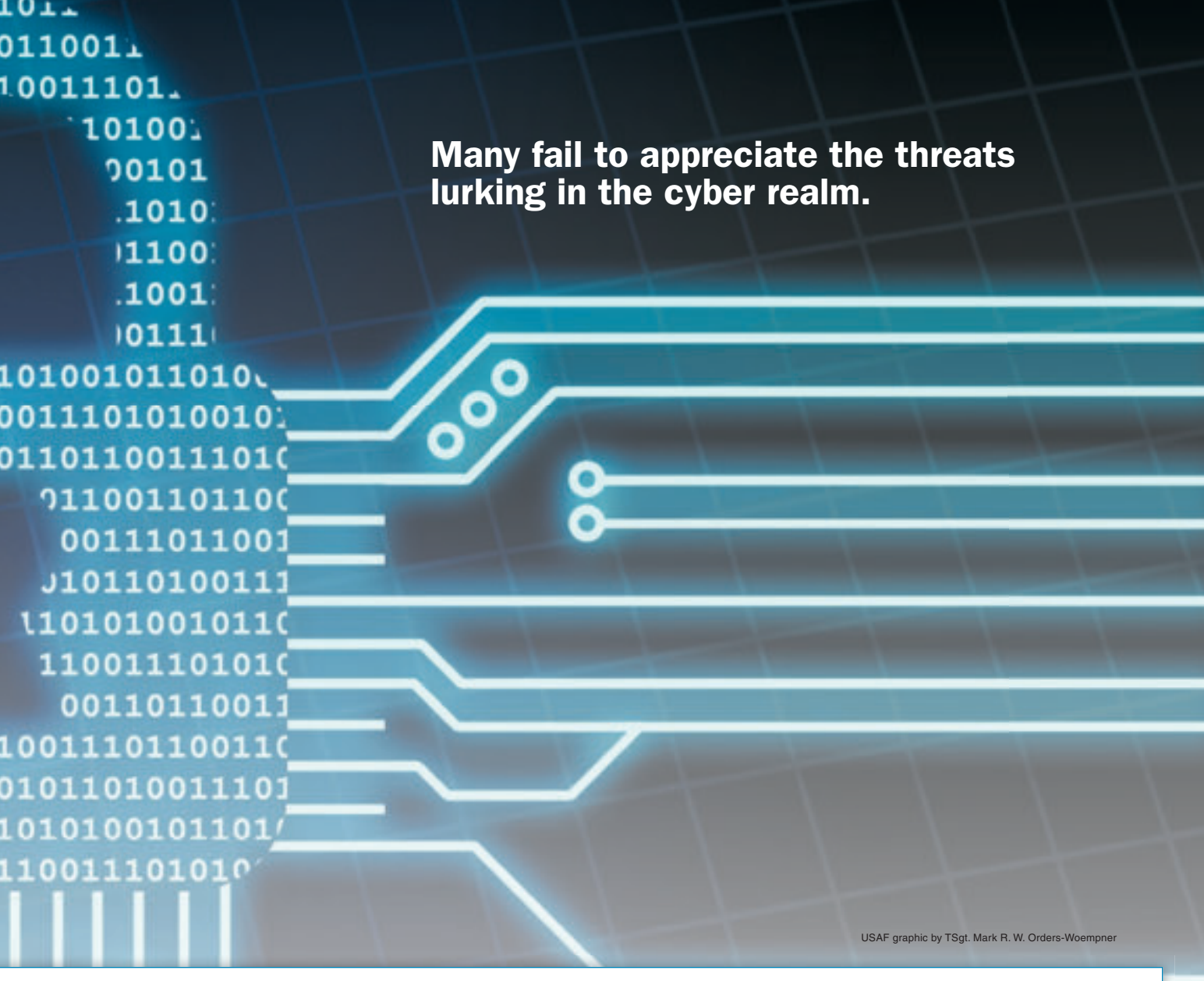
The Defense Cyber Crime Center, or DC3, operates under the executive agency of the Secretary of the Air Force with program oversight by the Air Force Office of Special Investigations. Among other functions, DC3 supports the defense industrial base through the defense collaborative information sharing environment, or DCISE, and supports law enforcement and counterintelligence organizations through the DC3 Analytic Group.

Private companies and defense contractors can send potential threats they find on their networks to DC3. The center then analyzes the threat, "sanitizes it to just the technology portion," and then shares it with the rest of the members of DCISE, said Christy. "People don't need to know who did it or why did they it. They just need to know the technology" so they'll know what happened and how to prevent it, he said.

Evolving Threats

Roughly one-third of the center deals with intrusions and national security matters, said the DC3 director, Steven D. Shirley, while two-thirds supports law enforcement and criminal investigations.

"When we receive evidentiary media from [an agency], we track it … by



Many fail to appreciate the threats lurking in the cyber realm.

USAF graphic by TSgt. Mark R. W. Orders-Woempner

assigning it an exam number," Shirley explained. DC3 then identifies and retrieves relevant information through "a reliable, valid, and repeatable empirical process." Basically, "others conduct investigations [and] we conduct digital forensic examinations in support of their investigations," he said.

In Fiscal 2012, the center supported 1,406 exams with 835 terabytes. In Fiscal 2013, DC3 ran 1,399 discrete and separate exams supporting investigations, running up 991 terabytes of data, an increase of 18 percent in data, though reviewing slightly fewer cases.

DC3's cyber analysts "develop a learning curve on different kinds of threats … so we have a substantial body of knowledge that we've [established]," Shirley said. "But at the same time, we see threats evolve in an increasingly complex and sophisticated, dynamic way."

During a Senate homeland security and governmental affairs panel hearing on Nov. 14, FBI Director James B. Comey Jr. admitted that he worries most about terrorism in the form of cyber attacks because it has become a metastasizing threat.

"With respect to cyber, whether by foreign governments or criminals or 'hacktivists' or terrorists, attacks on our computers and the systems that connect them have become one of the most serious threats to our nation," he said. He acknowledged that his predecessor, Robert S. Mueller III, warned him that threats from cyber attacks "would come to eclipse even the threat from foreign terrorism to our homeland" within Comey's tenure at the FBI.

"I believe that he is accurate in that prediction," said Comey. "We have connected, all of us, all our lives ... to the Internet, and that's where the bad guys will go because that's where our lives are—our money, our secrets, and our intellectual property."

Christy agreed with Comey's testimony but articulated that this concern has been around for two decades and nobody's really listened.

"It may be too late to defend [ourselves]," said Christy. "Before, when the Internet and the World Wide Web [were] just getting started, we could've built security into the systems but we didn't."

Christy said that it was probably because "nobody takes into consideration the bad people and how they're going to ... take advantage of that particular tool."

"We [just build to be] effective and efficient," he said.

Christy, who retired from DC3 last July, has since started his own consulting firm, the Christy Group, and will be hosting the US Cyber Crime Conference in April.

He ran the DOD Cyber Crime Conference for 12 years, but DOD scrapped the annual event in the wake of scandals involving excessive spending on lavish

conferences at multiple government agencies. So after Christy retired, he moved "to reincarnate that conference as the new US Cyber Crime Conference," he said.

One of the speakers at his upcoming conference will be Travis Reese, the president and chief operating officer of Mandiant, an information security company providing solutions to companies that have been hacked.

In a February 2013 report, Mandiant concluded from its investigations of computer security breaches around the world that the Chinese government likely sponsors advanced persistent threats that originate from within its borders. This was a revised position from what it had written in an earlier report stating that there was no way of determining whether the Chinese government was involved.

In "Exposing One of China's Cyber Espionage Units," Mandiant charged that the People's Liberation Army General Staff Department was aware of the attacks.

Mandiant focused on one particular advanced persistent threat group, saying "it is one of more than 20 APT groups with origins in China."

APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006, states the report. It went on to divulge three "personas" associated with the cyber activity: UglyGorilla, DOTA, and SuperHard.

The report grabbed the public's attention but "the government has known [about these attacks] for five to 10 years," said Christy. Still, he praised Mandiant for publicizing the information and creating awareness around the issue. He added that the government should take a larger role in disseminating this kind of information.

The government needs to change its tactics from merely informing the public after the fact to defending and protecting the public, and the best way to do that is with "some kind of offensive capability," he said. "Obviously they don't believe [cyber] is a big enough threat."

If America were under physical attack, it would defend its citizens, Christy said. But if an enemy comes at the United States virtually, the US doesn't do anything to protect the public, he argued.

The government, however, is showing some new signs of willingness to respond, and in one particular case last summer the government fought back.

Cybercrime Writ Large

Last July, the Department of Justice made public a federal indictment that was called the biggest cybercrime case ever to have been prosecuted in the United States, according to senior threat intelligence analyst Laura Galante. The US Secret Service headed the investigation on four Russians and one Ukrainian who were charged in New Jersey with conspiring in a worldwide hacking and data breach scheme.

"This is a really sophisticated group," said Galante, who works for Mandiant. The hackers stole more than 160 million credit card numbers targeting "corporate victims engaged in financial transactions, retailers that received and transmitted financial data, and other institutions with information they could exploit for profits," stated a July 25 DOJ release. The security breach was four times larger than the November/December 2013 credit card data theft from Target stores nationwide.

In the 2009 to 2013 data breach, the hackers attacked NASDAQ, 7-Eleven, Hannaford, JetBlue, Dow Jones, WetSeal, Visa Jordan, Global Payment, and a number of other vastly different companies.

Each member of the group had a specific role in the operation. Two specialized in penetrating network security while another specialized in mining the network. One used anonymous web-hosting services to hide the group's activities, and the fifth sold the stolen information.

Galante told *Air Force Magazine* that this operation "paints a picture of a more enterprise-like operation versus someone just sitting in a basement" and hacking from there.

USAF photo by A1C Kate Thornton

A1C Brock Metscher, a cyber systems operations operator, investigates a server configuration at Ellsworth AFB, S.D. Below left: Military members analyze an exercise scenario during Cyber Flag 14-01 in November at Nellis AFB, Nev. Gen. William Shelton, commander of Air Force Space Command, said he plans to commit more than 2,200 airmen to the cyber mission at 24th Air Force.

USAF photo by A1C Christopher Tam

An Air Force-led Cyber Center

Today's Defense Cyber Crime Center, based in Linthicum, Md., was created in August 1998 as an entity of the US Air Force. The center exists to support the Defense Department's law enforcement agencies and counterintelligence and cyber communities with digital forensics, training, and response to threats.

John J. Hamre, president of the Center for Strategic and International Studies, was deputy secretary of defense in the late 1990s when he authorized Air Force Office of Special Investigations along with the Defense Criminal Investigative Organizations' Enterprise-wide Working Group to create a set of programs. These programs became the Operating Location-Defense Computer Forensics Laboratory. The name changed to the Defense Cyber Crime Center in October 2001.

DC3 boasts of its own Defense Cyber Investigative Training Academy where it trains DOD criminal and counterintelligence investigators to run digital forensics and cyber investigations. It also houses the Defense Computer Forensics Laboratory, the world's largest accredited digital forensics lab, according to James V. Christy II, former director of futures exploration at DC3. More than a hundred examiners at the lab support criminal and counterintelligence investigations for the military's armed services and federal agencies. Criminal investigations can range from homicide, espionage, terrorism, to child pornography, Christy said. "It really runs the gamut."

Another worrisome detail in this case was the length of time the hackers had access to the network. The cyber criminals "had malware implanted on multiple companies' servers for more than a year, and they were waiting for months," Galante said. This "shows that they have the resources, the time, [and] the patience to sit and wait in these environments to get as much as they can out of that targeted incident. They're not just … grabbing a ton of numbers and leaving; they're doing this to maximize their financial gain."

Despite these mounting attacks in the cyber realm, Christy fears the Air Force is retreating from the cyber mission. Though there have been recent establishments of cyber-related entities, such as US Cyber Command and 24th Air Force-Air Forces Cyber in 2009, the Air Force has to start "cutting things and it appears that cyber is one of those that's going to be under scrutiny." That is especially so when coupled with budget cuts, sequestration, the rising cost of sustaining old aircraft, and the fact that "a lot of folks don't understand" the cyber threats, he said.

Air Force officials assert the service "has been a fully vested partner along with the other services to provide cyber capabilities to the warfighter," said Air Force spokesman Capt. Adam Gregory.

The Air Force works with the Army and Navy to organize, train, and equip personnel for cyberspace operations, and it "will continue to provide cyber capabilities and well-trained airmen to support the joint efforts in cyberspace," Gregory said.

At an Armed Forces Communications and Electronics Association event in December, Gen. William L. Shelton, commander of Air Force Space Command, told audience members he plans to commit more than 2,200 airmen to the cyber mission at 24th Air Force. Shelton also announced that as DOD moves toward a joint information environment, the Air Force has formed a partnership with the Army and Defense Information Systems Agency to consolidate its network security stacks into "joint regional security stacks" by early this year.

These security stacks "are designed to improve command and control and situational awareness, and are essential to enabling a single security architecture in the joint information environment," said Michael E. Krieger, the Army's acting chief information officer, last August.

As cyber threats—such as "denial-of-service attacks, malicious code, direct [attacks] on critical infrastructure, and theft of intellectual capital"—grow both in quantity and sophistication, Shelton said the US must "think very deliberately on how to counter these threats and how to ensure cyber mission accomplishment even in the face of attacks."

To effectively counter the myriad threats, the Intelligence Community, State Department, and DOD must use a range of responses and all of the different tools at their disposal, such as diplomatic or economic sanctions or overt and covert military operations.

Just as the government aggressively prevents a nuclear attack from happening, it should put as much effort into cyber, Christy said. ■