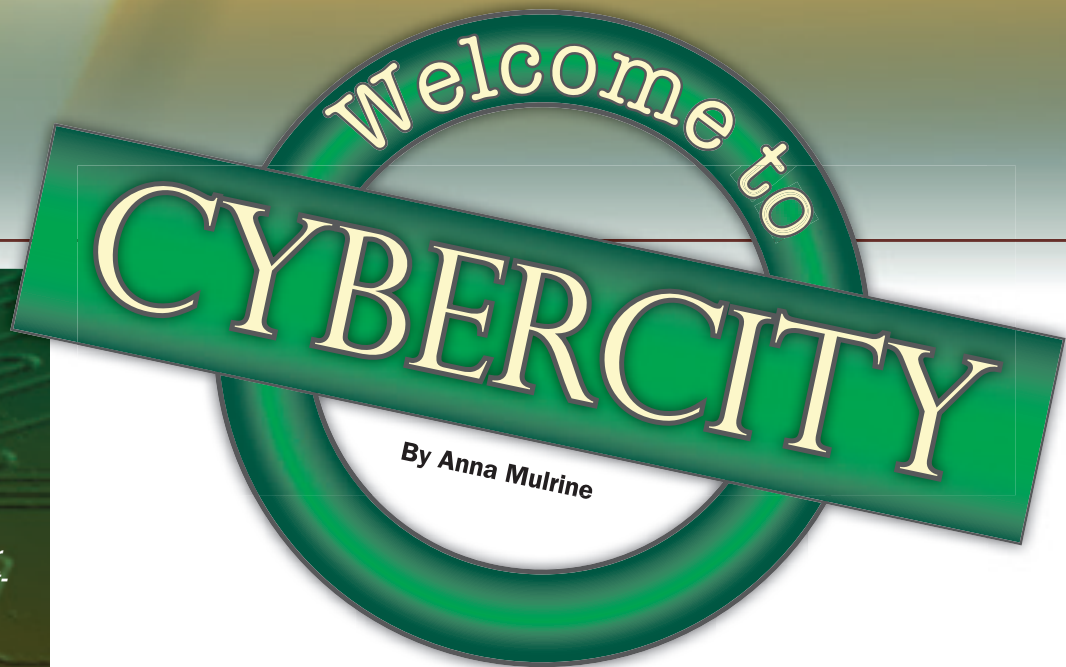


The Air Force's premier cyberwar simulator is used to train against a broad range of threats.




Photo courtesy of Ed Skoudis



Welcome to CYBERCITY

By Anna Mulrine



Ed Skoudis, founder of Counter Hack Challenges and a trainer at the SANS Institute, USAF's go-to organization for cyber training, with CyberCity, an eight-by-10-foot model of a "typical" town. The model is used to test cyber attack scenarios and responses.

In a nondescript region of eastern New Jersey, a train carrying radiological material is barreling toward a small town, and it is up to the Air Force to derail it. The town is the kind of idyllic whistle-stop hamlet where residents socialize in a cafe called Cuppa Jo (named after the town founder's wife) and enjoy free Wi-Fi while surfing FaceSpace, a social networking site.

But danger lurks all around. Terrorists have used the open Wi-Fi connection at Cuppa Jo to hack into the laptop of a doctor patron who works at the hospital down the street. They plan to use the hospital codes stored in his computer to access the medical records of the town mayor, where they will then change the dosage of a prescription he refills regularly in an effort to poison him.

The terrorists have other nefarious future schemes, too: They will cut the power grid with a nasty cyber virus and destroy the local water supply by engineering a cyber program to make the employees at the reservoir think it is polluted.

When the well-intentioned employees dump chemicals into the water to fix the problem, they will inadvertently be doing just what the terrorists want: contaminating the water supply.

The town is the US military's premiere cyber war simulator—CyberCity—and senior officials believe it has the potential to revolutionize the way the Air Force fights wars.

It is a city built with the help of a local hobby shop, complete with model

trains, miniature cell phone towers, and street lights attached to a power grid and spread out on an eight-by-10-foot table. It resides in the basement of the offices of Ed Skoudis, founder of Counter Hack Challenges, a company that designs cyber challenges, and a trainer at the SANS Institute, the Air Force's go-to organization for cyber training and certification.

CyberCity grew out of a request from senior Air Force officials—a request that offers some clues into what the force fears the most when it comes to cyber warfare and, in turn, the skills they desperately need to cultivate in the cyber workforce of the future.

It's clear that increasingly, for starters, officials fear that enemies will use computers not merely to steal secrets, but to manipulate power grids or supply line data, for example, to cause effects in the physical world—effects detrimental to US interests.

Real World Manipulation

"They came to us and said, 'We need you to figure out some way to teach cyber warriors that cyber attacks have a kinetic effect—that they make stuff move, blow up—that people can get killed,'" Skoudis says. "They were interested in having a reservoir. And they wanted a landing strip with lighting on it."

In short, "they wanted to get into cyber warriors' minds the idea that things can be manipulated in the physical world—it's not just stealing and exporting data."

Training a new class of cyber warriors is a Pentagon-wide endeavor. Senior de-



USAF photo by A1C Kate Thornton

A1C Micah Schrotberger, a cyber transport technician, troubleshoots an information transfer node port at Ellsworth AFB, S.D. The US military needs 20,000 or more cyber personnel to plan and combat cyber attacks.

that is something top Air Force officials continue to grapple with.

“We have not, in my opinion, fully cracked that nut yet,” says Lt. Col. John Weigle, commander of the 39th Information Operations Squadron, the Air Force’s information operations and cyber formal training unit.

Maj. Gen. Suzanne M. Vautrinot, commander of Air Forces Cyber and Air Force Network Operations at JBSA-Lackland, Tex., cites congressional figures that indicate that while the military has nearly 1,000 cyber warriors who can operate at the highest level, “what we need is on the order of 20,000 or 30,000.”

Boosting the Force

Even more than that, she adds, “Every airman has to have an understanding of cyber, because everything you do in your mission is dependent on it.”

In today’s force, “cyber is foundational to everything we do.”

The recent announcement within DOD that it would be boosting its force of cyber warriors is an acknowledgement of this point.

“It’s also a recognition that the problem has become so great that they need to act quickly,” says Alan Paller, founder of the SANS Institute. “And it’s recognition that in this arena, the skills are the weapon.”

fense officials are planning to boost the size of DOD’s cadre of dedicated cyber war specialists from 900 to 4,900.

Not only will these US troops protect computer systems, they also will include “combat mission forces,” according to defense officials, to help the command plan and execute attacks.

The challenge, however, also entails finding the thousands of qualified workers, getting them trained, and then retaining them in the armed forces. Just how to do

There are some particular personality traits that senior Air Force officials believe enhance these skills. “The biggest trait we’d like to see is curiosity,” Weigle says. “We need the technical skills, but also that curiosity about what’s around the next bend and that attitude that ‘I want to see it. I want to go do it.’”

In the quest to prevent and repel cyber attacks, rank matters little. “I’ve got very young troops that have done this since before high school, and they do scripting and computer stuff on weekends, too. This generation—well, I’ll say this up front, I’m extremely jealous,” says Weigle.

Indeed, at the highest levels, the military is becoming increasingly open about its growing need for the cyber skills of a young generation.

In order to train them, Weigle says that he would like to see the number of trainers in his command double “because some of the demands [from US Cyber Command] coming down from the services—we’re not able to pump out as many as they require over a five-year plan,” he says. “I could easily see this all doubling, given the correct instructors, to be much [closer] to what the nation needs.”

That said, there are limitations, Weigle acknowledges. “It all costs money, and my needs smack into the fiscal reality. They say, ‘Well, Colonel, that’s nice.’”

If the Air Force “has to take more operational cuts to feed the training piece, it’s a risk-reward type of function. So I can sit here as the training commander and say, ‘Yes, I need my staff to double.’ But at what expense, right? I do have to weigh that,” he says.



L-r: Petty Officer 1st Class Joel Melendez, USAF SSgt. Rogerick Montgomery, and Army SSgt. Jacob Harding analyze a scenario during Cyber Flag 13-1 in 2012. The exercise focused on DOD computer networks across the full spectrum of operations against cyber attack.

Cyber is a growing priority for DOD, which has become increasingly transparent about its need to grow these skills in the force—including offensive skills—about which the military has been close-lipped in the past.

The first major hint that this was happening began in the summer of 2012, with a request from the Defense Advanced Research Projects Agency (DARPA)—the high-tech arm of the Pentagon—for proposals to develop offensive cyber techniques.

Skoudis estimates that one-third of the CyberCity missions are designed to practice defensive skills, one-third to try to find vulnerabilities in the system, and one-third to hone cyber attack skills.

To illustrate the impact of these cyber attack skills, Skoudis has installed a miniature Nerf rocket launcher on the outskirts of CyberCity.

When the US military begins to use the cyber range regularly later this year, the mission for trainees will be to reverse engineer the controls to the rocket launcher to make sure it fires away from the hospital rather than—as terrorists would have it—toward innocent patients.

“If you can hack a computer and use it to launch a Nerf rocket launcher, you have some interesting skills, no?” Skoudis

USAF photo by SrA. Matthew Lancaster



asks. “The skills that we’re building can be used for offense or defense.”

Indeed, cyber warriors of the future often will need to deploy offensive skills to defend US interests, he points out.

“All the offensive stuff we describe is to take control of things to keep bad things from happening,” Skoudis adds.

“Of course, you can always use those skills to make bad things happen.”

Even though finding top cyber candidates has become a top priority for the military, the challenge has become to make the screening process sufficiently rigorous.

In some cyber training programs within the Air Force, even among airmen who have already shown a talent for cyber operations, there is a washout rate of roughly one in 10, Vautrinot says.

Five years ago, the screening process for cyber warriors got so tough that no one could pass the tests, says Paller of the SANS Institute. But then there was the danger of a ricochet effect—in other words, of making the screening tests too easy.

“Because it was hard to build this talent, the danger was that the military could fall back and send up not-so-qualified people.”

Left: CyberCity is equipped with miniature buildings, model trains, cell towers, and street lights attached to a power grid. Officials fear that enemies will use computers not only to steal secrets, but to manipulate power grids or supply lines.

Photos courtesy of Ed Skoudis



Today the Pentagon is building “phenomenal training programs in advanced cyber skills,” says Paller. “The big idea there is a talent search within the existing military forces.”

The National Cyber Range developed by DARPA, for example, allows cyber specialists to quickly replicate real-world incursions in a variety of networks—from top secret to open. It then times their ability to identify the source of the attack and quickly shut it down.

In the past, many cyber training programs have involved a “king of the hill”-style approach. That means that “two percent of the players do very well and get to the top of the hill,” says Skoudis. “And then they push off the rest.”

So while it’s possible to find the very top cyber warriors, it’s difficult to rank the rest, he adds. The emphasis now is to more clearly find ways to assess the skills of cyber warriors. “One of our big focuses” has been to find ways to separate players into fifths, says Skoudis. “You want to know who’s the best, but also who are the rest in the first quintile, and who’s in the second quintile—those people are also very interesting.”

Gradually, more pipelines into the military are opening up to try to bring more talent into the cyber corps.

The 39th Information Operations Squadron, run by Weigle and located at Hurlburt Field, Fla., has the only simulator in cybersecurity in use, which is helping to build training programs in advanced cyber skills, in much the same



USAF photo by SSGT. Christopher Boltz

Maj. Gen. Suzanne Vautrinot, head of Air Forces Cyber, fears sequestration will hurt recruiting for cyber specialists. Before the budget bludgeon, talented civilian cyber gamers were brought in for a temporary stint—something that may be forbidden under sequestration.

way, Paller adds, that the US military trains fighter pilots.

The military also has begun adding considerably to the cyber course offerings, and the services are reaching out to high school-aged students in the form of talent searches.

Thousands of schools throughout the country are building cyber game teams, with mentors from across industry and the military. Cyber training companies are building games to assess individual skills, too. The Air Force Association's CyberPatriot program has gained national prominence and engaged more than 1,000 teams each of the past two years in the nation's largest high school cyber defense competition.

"You've got to find a way that reaches to the individual, so if you compete well, there's a recognition that you do really well in those skill sets," Vautrinot says. "They highlight you to the industry, 'Hey, this guy's got game.'"

Students who have caught the eye of commanders for their skill in cyber games are recruited into an internship program to do temporary stints in Air Forces Cyber and are given security clearances as well. "We gave them clearances and they were actually doing forensics on intrusions into our network," Vautrinot says. "It's like that game tape: How did that work so I can thwart it the next time?"

This tends to involve heuristics, she adds, expanding on the sports analogy. "What does it look like when they move back their arm to throw? So that even before the play sets up it can be identi-

fied and automatically responded to on the network."

These skills, in turn, help the students' participation in the games: Last year's winning team was made up of interns in Vautrinot's cyber emergency response team. "Early engagement is vital for closing the gap," she says.

There have been some hiccups, however—Vautrinot worries that sequestration will keep Air Forces Cyber from recruiting at least one class of top students because of its prohibitions on hiring temporary employees. "A couple" of the interns from these programs have come into the Air Force so far, Vautrinot says, emphasizing that "this is about rising tide, all ships."

Holding On

Keeping talent can be just as difficult as finding it in the first place. Once the Air Force provides the recruits with the necessary skills, the problem is that they are very valuable to industry and have often been recruited away. While the concern is getting qualified troops to fill the growing demand for cyber professionals, it can be a problem when it comes to retaining top trainers, too.

Retention "is a big concern, to be honest, and all the more so for my instructors," says Weigle. "The best cyber pros out there are instructors." He recalls some recent employee losses. "We let them go with the gnashing of teeth, as we do," he says. "It's an issue—one that we all take very seriously." That said, he adds, there is "extreme job satisfaction in turning out the next generation."

Weigle recognizes, however, that for instructors "the incentive is not only to do good things, but also to put food on the table. I can't fault a guy or gal who has an offer." If they are "exporting" their skills into industry, "that's OK, too. We're giving this person up to go out in industry, but he boosts it up. We all rise with the tide."

There has been some discussion about whether there should be a two-tiered track of sorts for cyber specialists. Because they often work back in garrison,

for example, maybe they don't need the same physical skills that, say, infantry troops have.

"I've heard that: 'Why do I need to be able to shoot straight and run a mile-and-a-half in 10 minutes?'" says Weigle.

But many officers remain skeptical of troops who don't also meet the physical requirements required of everyone else in the military.

"One of the insurmountable things in the military is [that] the way you rise is through acts of valor, wielding weaponry in the traditional sense—bullets, bombs, planes," Skoudis says.

While civilian analysts like Skoudis acknowledge that "from a military perspective, to gain respect, you need the discipline to wake up early in the morning, for example," he also believes that "creating a dual track is vital."

So, too, is a sense of respect for the work the specialized troops do. The force is increasingly acknowledging the role that cyber specialists play in national security, most recently with the proposed creation of the new Distinguished Warfare Medal, created in part for distinguished acts in the cyber realm. "Since Sept. 11, 2001, technological advancements have, in some cases, dramatically changed how we conduct and support combat and other military operations," said Defense Secretary Chuck Hagel. "It recognizes a specific type of contribution that is vital to the defense of our nation."

But even the Distinguished Warfare Medal got caught up in the debate about what represents valor and what is vital in the military. Bowing to concerns, DOD killed the medal, opting instead to create a new distinguishing device to affix to existing medals in order to recognize military personnel such as cyber operators.

Still, the new device is "an acknowledgement of the fact that the military knows that cyber is a critical role now. In the new ways that wars are being fought, drone operators are more important now than ever," Skoudis says. "In fact, they can take actions that can save thousands or hundreds of thousands of lives. They are not specifically on the front lines, but the actions they are taking impact the front lines directly."

"It shows the military knows that to retain these folks, they need respect. And the military is increasingly giving it to them because they are earning it." ■

Anna Mulrine, a staff writer for the Christian Science Monitor, reports frequently from Iraq and Afghanistan. Her last article for Air Force Magazine, "Seeking the Sex-Assault Solution," appeared in April.