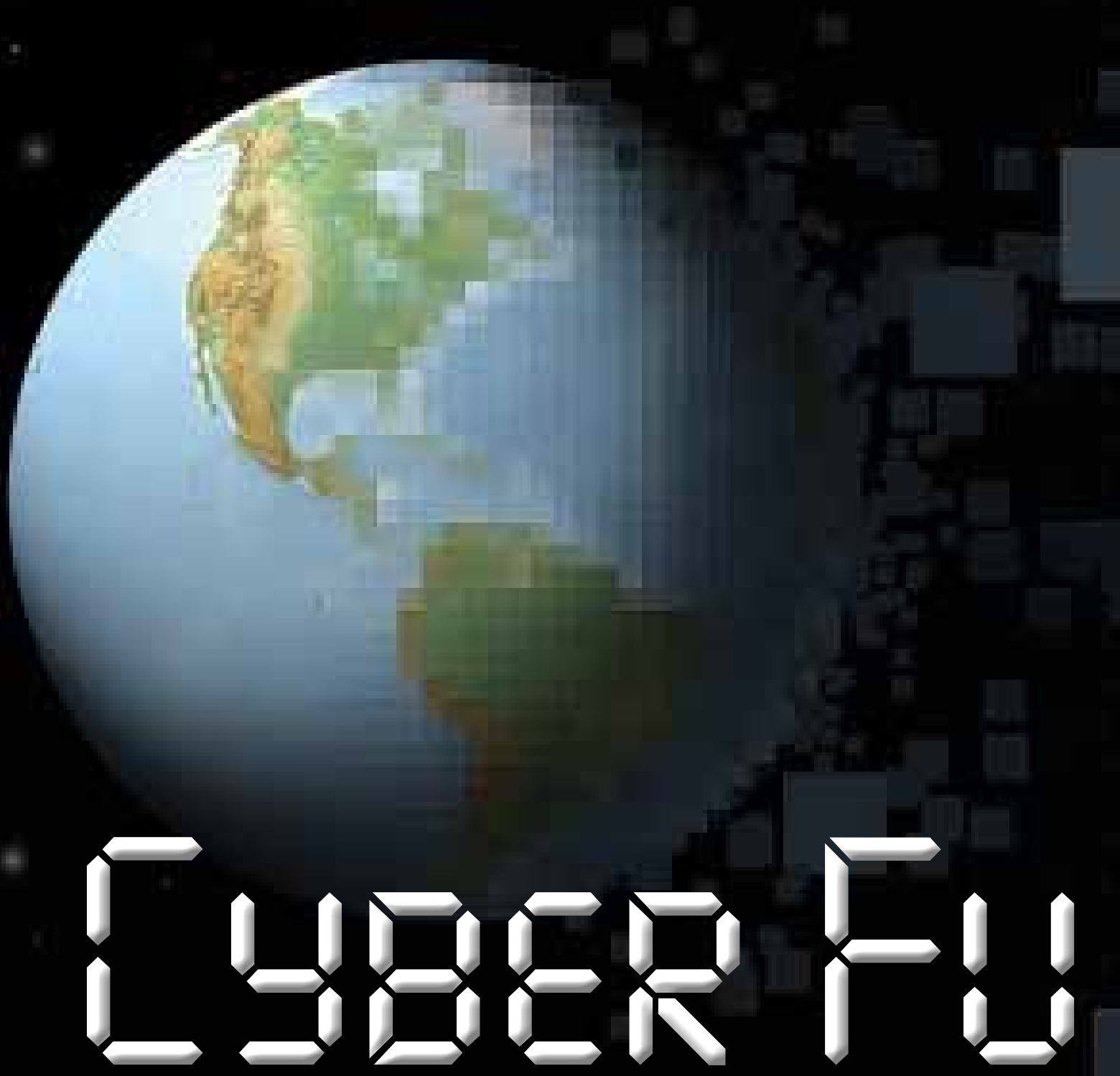
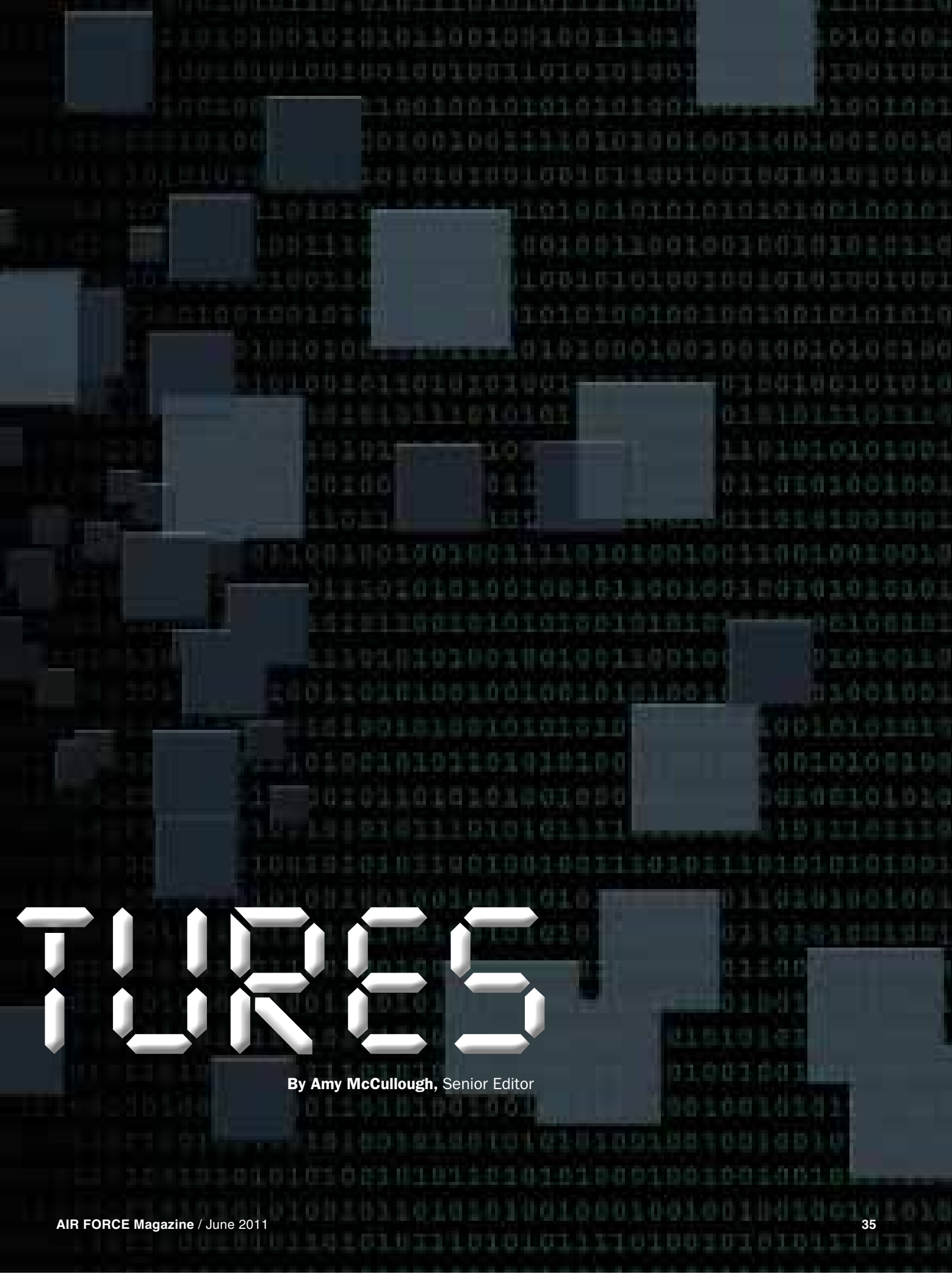
At AFA's first-ever CyberFutures conference, top officials spoke of the need to prepare for war in cyberspace as they do for air, land, sea, and space.



Cyber Fu

Staff illustration by Zaur Eylanbekov



TURES

By Amy McCullough, Senior Editor

One of Air Force Space Command's top priorities is to operationalize and normalize military cyberspace. The task is difficult because few people understand the laws and principles surrounding the Defense Department's newest operational domain—which is entirely man-made.

Cyberspace is constantly changing and many of the fundamental questions, such as whose job it is to guard the networks and how that will be accomplished, remain unanswered. Nonetheless, AFSPC officials hope to speed up the process by pulling from 20-plus years of lessons learned operationalizing the space domain.

Building the cyber workforce and establishing the necessary authorities will be key, but these also pose some of the biggest challenges, said officials at the Air Force Association's inaugural CyberFutures conference held March 31 to April 1 in National Harbor, Md.

"The one guarantee in today's cyberspace domain is that it will be different in the future," said Lt. Gen. Michael J. Basla, vice commander of Air Force Space Command. "In the physical domains, the laws of nature never change. We can count on gravity as a constant. In the cyberspace domain, the rules of humans dominate and we can't count on that stability."

Although the people, products, and ideas underpinning cyberspace may be a bit more mature, the field itself remains in its infancy and still lacks a "coherent, higher level framework" to guide investment, said James Richberg, the assistant deputy director of national intelligence for the cyberspace office of the Director of National Intelligence. Richberg helped develop the Comprehensive National Cybersecurity Initiative, launched by President George W. Bush in January 2008.

USAF photo by SSgt. Tiffany Trojca

Air Force Chief Information Officer Lt. Gen. William Lord addressed threats to the Defense Department's network at the Air Force Association CyberFutures Conference at National Harbor, Md.

Whack-a-Mole

The CNCI now plays an integral role in implementing the recommendations of President Obama's Cyberspace Policy Review, which includes creating a unified response to future cyber incidents, strengthening public and private partnerships to find technology solutions that ensure America's security, and investing in cutting-edge research and development in the cyber domain.

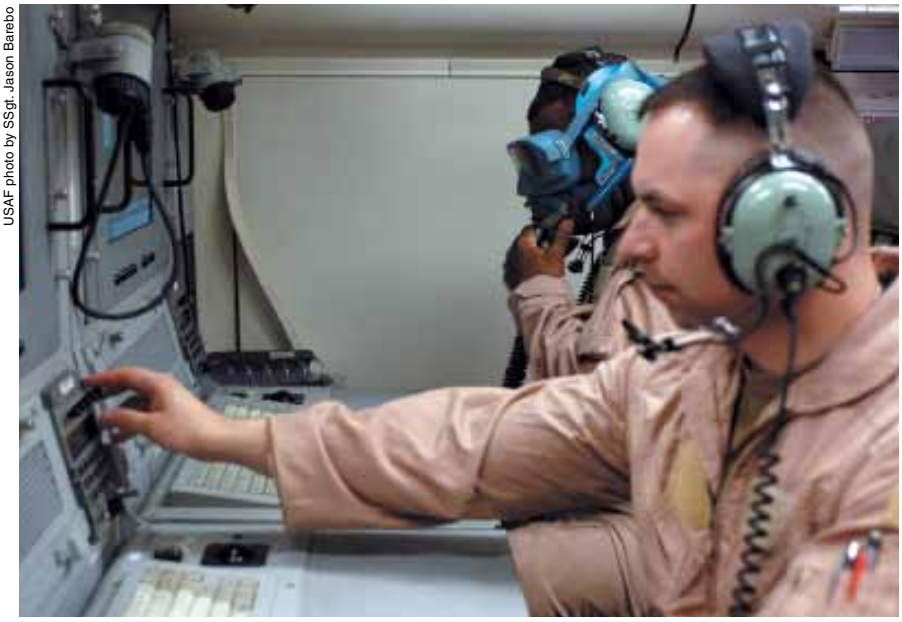
Richberg said there needs to be a "scorecard" that the government and private sector can use to check off successes and inefficiencies in cyber. Rather than living with hardware and software that are incompatible or bugs that may or may not be fixed, Richberg said officials need to seek some type of performance warranty, much like you get when you purchase a new automobile.

Estimates show that the public and private sectors spend more than $20 billion annually on cybersecurity. The Pentagon's Fiscal 2012 budget request includes $4.6 billion for cyber in the Air Force alone—the same amount set aside to fix the F-35 strike fighter program.

Yet, "we are still playing whack-a-mole on threats," Richberg said.

"Few of us would buy a plot of land and then head to the neighborhood home improvement store to buy supplies to build our own house without blueprints, yet that's the way much of enterprise IT architecture sprang up," he said. "So, in terms of guarding the networks, it frankly isn't surprising that most customers end up with a la carte cybersecurity solutions and little to no system integration or idea of security performance."

The Air Force network has been scanned thousands of times this year, including 132 suspicious events and 10 new malware signatures, said Lt. Gen. William T. Lord, USAF's chief



USAF photo by SSgt. Jason Barebo

USAF Capt. Stefan Essig (r) and Army Maj. Darryl Verrett run computer systems checks aboard an E-8C JSTARS. The Pentagon and combatant commands continue to discuss roles and command and control in the cyber realm.

of warfighting integration, during his address at the conference.

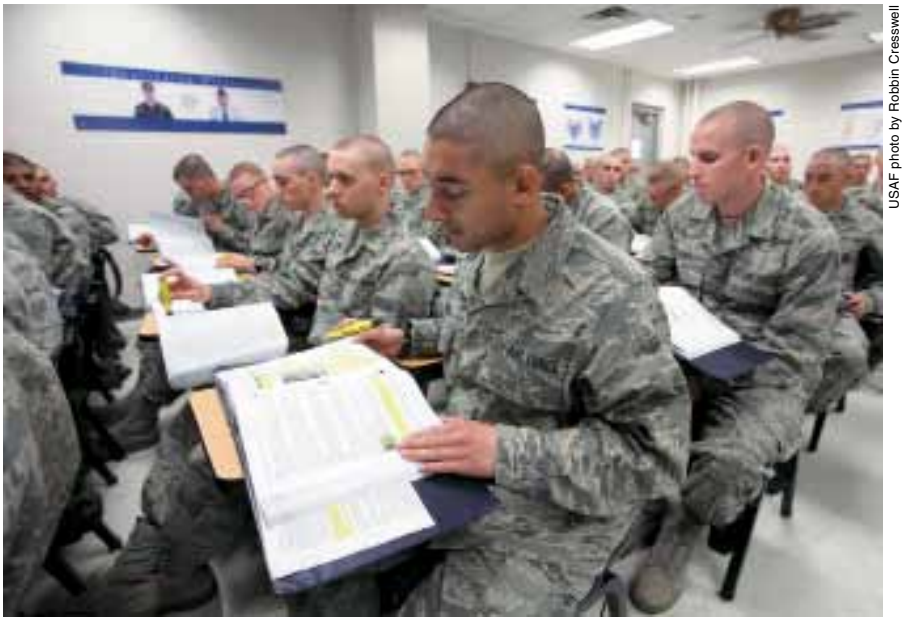
Those threatening the network are after the Pentagon's intellectual property and proprietary information, but "most importantly, ... they are accessing our networks for later exploitation," Lord said. The hackers and attackers trying to gain entry into DOD networks also are becoming more and more sophisticated. If compromising the network becomes too much of a challenge, Lord said they will simply move on to one of the 19,000 applications on the USAF network—each of which has a varying degree of security.

That's why the Air Force is putting its applications through rigorous testing to fix holes in the system. However, technological advances and plugging holes are not the only solution. The government will never be able to keep pace with cyber developments; chasing technology will always be an uphill battle, Basla said.

Though Basla said he doesn't want to "discourage innovation," the best way to create the stability necessary to operationalize and normalize cyberspace is through "deliberate processes while developing our people."

A true fix will require changing the culture in the Air Force so the cyber cadre is trained with the same operational rigor as those working in the air and space domains.

"We're getting there but we're not there yet," Lord said. "In an operational weapon system, ... I'll bet you don't just walk in there and tear off the shrink-wrap that came with the commercial product and click, click, click until it doesn't work. We're changing the way that we train, certify, inspect [those] ... who are running our networks today. That's cultural. That's training. That's educational."



USAF photo by Robbin Cresswell

Air Force basic military trainees learn about defending cyberspace during a class. USAF leaders say training in the cyber domain is just as important as training in the air and space domains.

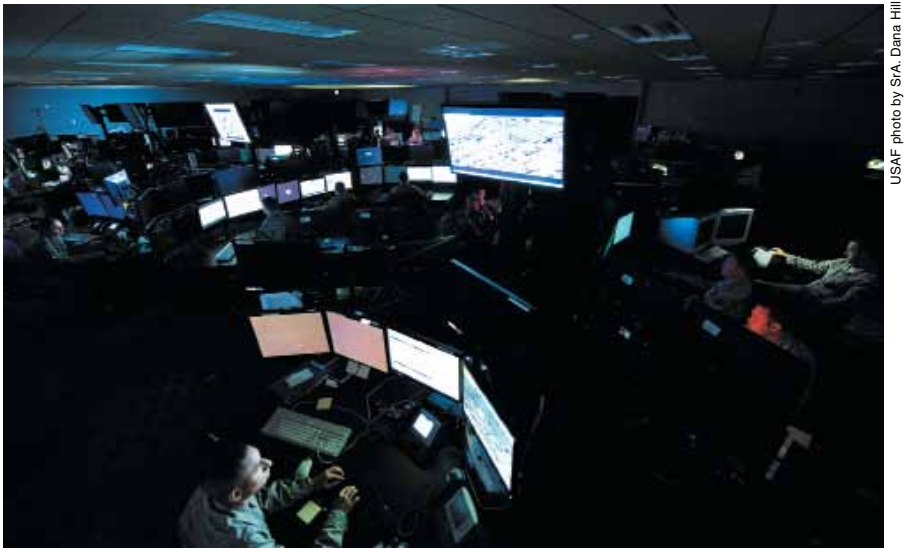
The Trouble We Have

Lack of training is the No. 1 way to remain vulnerable, said Air Force Maj. Gen. Ronnie D. Hawkins Jr., vice director of the Defense Information Systems Agency. Hawkins suggested all senior leaders should be certified to operate on the network, just like an F-16 pilot is certified to fly the aircraft. Re-engineering the workforce has to start at the top and then work its way down to the lowest ranking airmen, he said.

The Air Force would not allow someone to command an aircraft wing if he didn't know how to fly that aircraft, so it should not allow people to work within the cyber domain without first becoming certified to do so, Hawkins said. There also needs to be an additional layer of scrutiny of the information that is allowed into the cloud. That could mean decertifying people if they screw up and prohibiting them from operating on the network until they can go through the proper training, just as pilots can be decertified following an accident investigation review board.

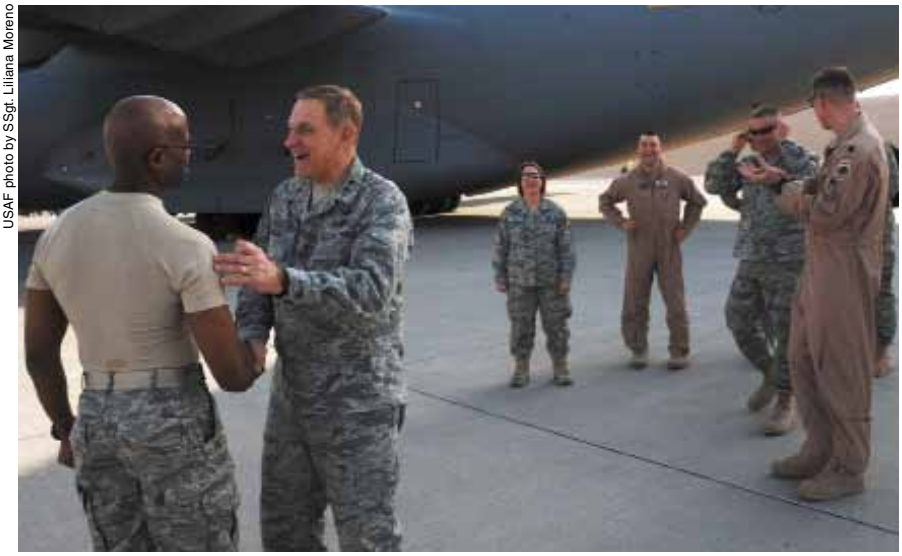
"None of us would get on an aircraft ... with the knowledge that the pilot and everybody on that aircraft had not been certified and also recertified at some time or another," said Hawkins, who said operating in cyber should be no different. "Until we get there, we're going to have the trouble that we have. We're going to have the intrusions that we have. And more importantly, we will not be able to gather the right type of information to effect the change that needs to go on to secure the cloud and more importantly secure cyber."

Cybersecurity will require a well-trained and experienced cadre. The best way to grow and train the force is to align a collection of relevant career fields under one cyber force, said Maj. Gen. David N. Senty, chief of staff for US Cyber Command. That would mean those building the network, doing combat communications, network defenders, and cyber operators would move through the same stovepipe, and



USAF photo by SrA. Dana Hill

Airmen with the 497th ISR Group work on the operations floor at JB Langley-Eustis, Va. Industry leaders say they are already seeing a convergence between the Intelligence Community and the IT experts.



USAF photo by SSgt. Liliana Moreno

Maj. Gen. Michael Basla, now Air Force Space Command vice commander, greets Maj. Gen. Edward Bolton Jr. (in t-shirt), director of cyber and space operations at USAF headquarters, while touring a flight line in Southwest Asia. At AFA's cyber conference, both spoke about the challenge of operating in a domain that is constantly changing.

the Defense Department would be able to pull from each of those skill areas to best protect the network.

DOD also is trying to find a "logical career track" for the next generation of cyber warriors. Senty said it would be a "special operations-like career field" made up of "a skilled, selected, distinctive cadre that can operate in cyberspace with the same [confidence] as our combat arms and operators do today."

These cyber commandos would have backgrounds in intelligence, space operations, engineering, electronic warfare, combat arms, and especially planning. Planners will play a key role in maneuvering through the intricacies of cyberspace and integrating "at all phases of an operational plan," he said.

The goal is to build a multidisciplined workforce, where the cyber cadre is first trained at US Cyber Command and then goes off to work under the National Security Agency and/or DISA before coming back into their respective services, each bringing with them a wealth of new knowledge.

To make the network "smarter and more secure," DOD needs to create an ebb and flow within the community that allows the cyber cadre to easily move from one career field to another. This will ensure they remain in touch with the cyber domain throughout their careers. In this model, those trained as network builders could find themselves at some point acting as cyber hunters who chase down "spurious data, unusual behaviors, or anomalies" in the network, Senty said.

Barbara G. Fast, the vice president of cyber solutions for Intelligence and Security Systems, a division of Boeing's Network and Space Systems, said she does not believe cyber will remain a niche career field. In fact, the transition to a more permanent career path already is taking shape and it's bringing with it a convergence between the Intelligence Community and the IT experts, said Fast, a retired Army major general.

Army Gen. Keith B. Alexander, commander of USCYBERCOM, may be the first senior cyber officer but he won't be the last.

Setting the Standards

"That is going to be the largest core operational competency because it is inherent in every mission that we perform. It's how we operate today," Fast said. "We sometimes tend to think of it, particularly in industry, as being at the enterprise level, but more and more, it's going to migrate ... to the tactical edge."

Successfully creating that long-term cyber workforce will require heavy investment in education, said Robert F. Brammer, vice president for advanced technology and chief financial officer for Northrop Grumman's Information Systems sector, because building a broadly based cybersecurity workforce is a critical national security issue.

"We're beginning to realize the importance and what it would take to get that done. ... I know we're making progress, but I also have a very healthy respect for how much more there is to be done," he said during an industry panel discussion at the conference.

Lynn A. Dugle, Raytheon president of Intelligence and Information Systems, agreed that education is crucial, but said industry is too reliant on traditional learning methods and processes.

"I am extremely confident that if I went to many of my colleagues who are generals and I said to them, 'Sir, we're going to enter the battle tomorrow. We are outmanned one-to-10, one-to-12,' ... I don't think [their] response would be, ... 'We're going to create a four-year college curriculum and we're going to fill the gap," Dugle said. "What I'm saying is not anything against well-thought-out programs, ... but I'm saying that it's insufficient. ... Not only because [it takes] too long, but in this field, dynamic learning is the name of the game. [Cyberspace] is not like physics. It's not like civil engineering where what you learn has a half-life of decades."

As the education process accelerates and evolves, government and industry will have to come up with a uniform definition of success. Today, there are many metrics to gauge cybersecurity, such as money spent, pieces of malware blocked, percentage of audit compliance, but there are few "real measures" of success, said Richberg.

Determining what constitutes the appropriate level of cybersecurity is not an easy task, because what is considered adequate security in one context may be unacceptable in another, he said. For example, it's not likely the government would accept anything less than zero defects when talking about the security control system for a nuclear power plant. On the other hand, the standard likely would be less stringent when talking about cyber crimes.

The key to protecting the networks will require an open dialogue based on a standardized vernacular and shared framework, plus a common model to drive the roles and responsibilities of all parties involved in the cyber domain. Richberg offered a general paradigm based on detection, defense, resilience, and recovery.

The orientation of malicious cyber activity, or attribution, would fall under detection in Richberg's model—something he called either the "Holy Grail or the Achilles' Heel of our field, depending on whether you are an optimist or a pessimist." Cyber defense would include coverage of everything from the common desktop computer to the entire enterprise network. Resilience, in this case, can be defined as damage limitation, while recovery is the ability to generate a replacement capability if attacked.

Whether you buy into his proposal, Richberg said "a successful model, ideally, should be readily understood by the laymen, help practitioners map where their particular focus is relative to the big picture, and can help describe or even define those roles and responsibilities for individuals, enterprises, and governments."

Hawkins, the DISA vice director, said the Pentagon needs to "start reducing the attack surface" from which cyber threats can come. By reducing such noise, cyber warriors can focus on specific areas of interest, build partnerships, and increase discipline, he said.

"We do a lot of information sharing. We do very little collaboration. We do a lot of reactive work. We don't do a lot of work on the front end," said Hawkins. "But there is a lot of intellectual capital. There is a great deal of information that is out there concerning the threats, as well as the tactics, techniques, and procedures to inoculate our different networks such that they would not be attacked or would not be penetrated. And if they were and are, we would be able to do something about it."

Until that collaboration becomes common practice, though, the cloud enterprise will always be vulnerable because you never know when an attack is going to take place, Hawkins said.

The focus now is on "breaking down the silos" between each of the services and federal agencies that need to come together in this new domain and figuring out how each one fights and operates in cyberspace.

There has been an ongoing, "intense" discussion between the Pentagon and the combatant commands about key terrain and command and control, Senty said.

While COCOM commanders look at cyber from a tactical perspective, Cyber Command takes a more strategic approach. The goal is to balance the two, so commanders can be confident that the latest technology will be available to aid them in the fight when and where they need it.

The cyber terrain is not so different from the physical battlespace. It includes physical maneuvers, lines of approach, and various ways to array military forces.

"We think of the cyber terrain in a similar format but mapped differently; key terrain features, avenues of approach, defensive positions, extraction points, exfiltration points. How to look at things at a strategic, operational, or tactical level may lead you to a specific point on a network, and our objective in this case is to inject ourselves in the right place in a process for maximum utility, maximum military utility," he said.

In the future, cyber operations, kinetic operations, and intelligence will merge—a process already under way, said Maj. Gen. Edward L. Bolton Jr., director of cyber and space operations at USAF headquarters.

Developing Specialists

Sometimes a cyber offensive attack will be a smarter solution to what would traditionally have been conducted as a kinetic operation. Israel's 2007 attack on Syria's integrated air defense system, which was the biggest and supposedly the best Russian-made system at the time, is the perfect example. Instead of kinetically taking out the Syrian IADS, Israel hacked the network, flew in undetected, and then bombed a nascent nuclear facility.

"You're going to see, and you're already seeing, a trade-off in options between kinetic and nonkinetic attack," said Bolton.

Air Force officials expect to see an "exponential change" in the type of users operating in the domain. Right now, more than a third of the users live in Asia, and China will prove to be a formidable opponent, said Bolton. The Chinese are developing cyber specialists in the same way the Soviets once developed athletes.

"They take the best 50 or 60 kids in a school who are good at math and give them computers. Those kids have a runoff. The No. 1 kid goes to a special school. Those kids have a runoff," said Bolton, who said it won't be a stretch to see "half a million Chinese scholars" trying to break into the Pentagon's networks within this decade.

Though China's prominent role in cyberspace is not new, Bolton said he expects to see a spike in the number of currently undeveloped countries participating in the domain. "The slope of the curve on the less developed world is actually very, very sharp, so you're going to see a dramatic increase," he said.

The future of cyber also will rely on smart data to create a secure cloud, where the user's identity is valid and identified. Keeping track of mobile users and maintaining strong encryption on such devices presents a significant challenge, he said.

"Something we protect at Cyber Command is our networks, [but] we're also protecting privacy and individual rights," said Senty. "It's a technology challenge that I think our country needs to address because of our adherence to doing those two things simultaneously and not compromising one for the other." ■

A Man-made Realm With Real-World Effects

Maj. Gen. Edward L. Bolton Jr., director of cyber and space operations at Air Force headquarters, said future battles will merge cyber operations, kinetic operations and intelligence—and the synergistic process has already begun. In the cyber domain, an adversary may find a nonkinetic means to defeat an enemy.

In 2007, as a prelude to bombing a Syrian nuclear facility, Israel disabled Syrian air defenses through a cyber attack.

Also in 2007, Russia was accused of unleashing a cyberwar on Estonia. The three-week cyber assault disabled the government ministries website, as well as the websites of Estonian political parties, banks, and various newspapers. The electronic onslaught continued until NATO got involved to help beef up the Alliance member's cyber security. The attack on the small Baltic country is the first known incident of such an assault on a nation-state.

The next year, before Russia invaded Georgia in August 2008, Russia first conducted denial-of-service attacks on Georgian news and government websites. As hostilities ramped up, so did the severity of the cyber attacks. They eventually forced Georgia's entire banking system to shut down, as banks attempted to protect themselves and prevent the loss of confidential data. The attacks essentially isolated the country from the rest of the world during the early days of the war.

But cyber threats are not always intentional. Air Force Maj. Gen. David N. Senty, chief of staff for US Cyber Command, said one of his biggest concerns is that a simple click of the mouse will lead to catastrophic physical destruction of property, as it did in Siberia in 2009. One of the operators at the Sayano-Shushenskaya hydroelectric power plant completely destroyed the facility and more than 70 people died after he accidentally activated one of the power plant's turbines that had been taken off line.