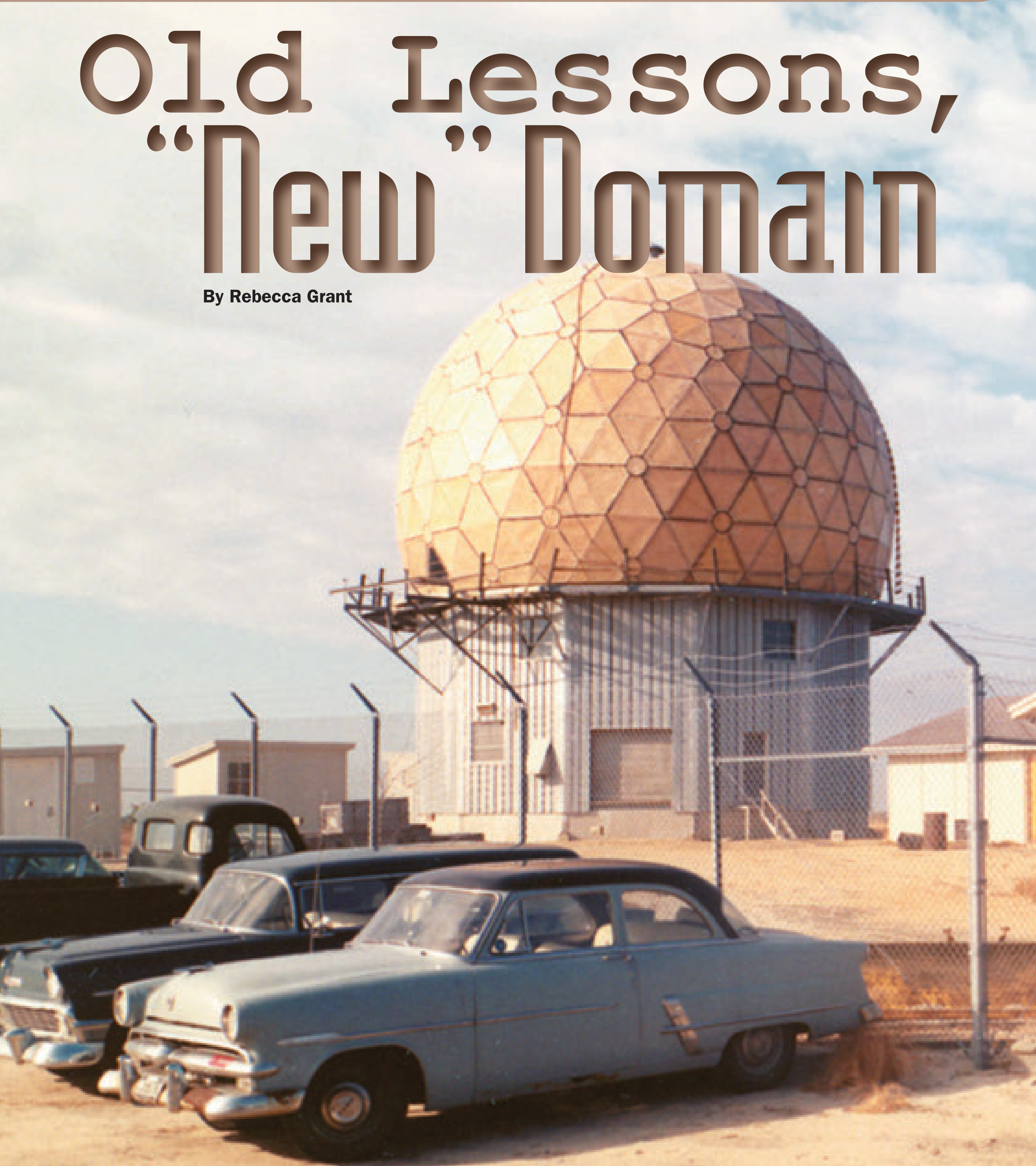
The Air Force can learn a lot from what it has already seen in cyberspace.

Old Lessons, "New" Domain

By Rebecca Grant



Cape Cod radar tower in Massachusetts was a prototype for the SAGE air defense system. SAGE needed computers with memory, digital relays linking radar sites, and systems engineering to bring them together.

Photos via MITRE Corp.

Washington is once again wrestling with how to tackle the military challenges of cyberspace. "The rise of cyber is the most striking development in the post-9/11 national security landscape," Chairman of the Joint Chiefs of Staff Army Gen. Martin E. Dempsey said in a June 27 speech at the Brookings Institution. Dempsey said about 4,000 new military cyber positions could be created. Perhaps 1,000 of those may be within the Air Force.

Responding to new growth in the cyber mission poses a challenge to the Air Force. Over the past decade, the USAF position has swung from taking a vigorous lead in the mission area to going slow on cyber—to avoid a potential "black hole" as Air Force Chief of Staff Gen. Mark A. Welsh III termed it in late 2012.

As the debate continues, it is important to recall that cyberspace is not new territory for airmen. The Air Force made its first deliberate move to create a cyber force structure almost 20 years ago.

"The longer we think cyber conflict is new, the more we will repeat the same mistakes and relearn old lessons," wrote Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic Council, in Air University's *Strategic Studies Quarterly* in fall 2012.

Cyber lessons mark out a heritage every bit as interesting as biplanes and bridge bombing. In fact, USAF can look back at six decades of involvement in the domain now called cyberspace. Air Force strategic challenges, such as continental air defense in the 1950s and real-time command and control in the 1980s, fueled progress in the exploitation of cyberspace.

In its infancy, the domain of cyberspace did not look much like the clouds and commons known around the globe today. The special qualities of cyberspace emerged only when computers gained more memory and power and networks linked them together.

In the (Cyber) Beginning

Back before social media, the World Wide Web, the first emails, and even before ARPAnet, the first closed cyberspace system was the Air Force's Semi-automatic Ground Environment, or SAGE.

The Air Force bought and paid for SAGE, which was arguably the first true cyberspace environment.

SAGE's intent was to direct continental air defenses to intercept attacking Soviet bombers. From 1949 on, the entire United States was vulnerable to nuclear attack from Soviet bombers refueled near the Arctic Circle.

The defensive problem had grown too complex and immense for the grease pencil and telephone line methods of World War II to remain effective.

MIT professor George E. Valley Jr. dove into the problem as a member of the Air Force Scientific Advisory Board. Valley visited an air defense site in Massachusetts and was horrified by the old equipment and procedures.

An early "cyber warrior" in 1959 uses a light gun to target potential intercept coordinates.

The Morris Internet Worm
source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

The Computer History Museum

Museum of Science photo via Wikipedia

Austin Mills photo via National Cryptologic Museum

Above: The disk containing the 99 lines of code comprising the Morris worm. Right: Frostburg, a supercomputer programmed to perform higher-level mathematical calculations for the National Security Agency, operated from 1991 to 1997.

Valley briefed Air Force Chief Scientist Louis N. Ridenour, who then persuaded MIT President James R. Killian Jr. to establish a new laboratory at MIT and use Air Force money on air defense research. They also hoped to stimulate the information electronics industry.

SAGE was a unique step toward cyberspace because the system was conceived from the beginning as an information architecture. “SAGE was one of the first systems to include immediate, interactive man-machine communication via displays, light guns, and switches,” noted a 1974 RAND report on future USAF command and control software requirements.

To work, SAGE needed computers with memory, digital relays linking radar sites to command and control nodes, and systems engineering to bring them together.

Air Force requisites for SAGE carved out many of the tools for cyberspace. First was a fast computer with programmable memory. The MIT campus had a computer known as Whirlwind that could receive radar data and respond with an intercept path in real-time, thanks to its nascent electrostatic random access memory and programmable read-only memory. The Air Force took over funding of the computer from the Office of Naval Research.

Digital computer maturation in the SAGE project “laid the foundation for a revolution in digital computing, which subsequently had a profound impact on the modern world,” summed up MIT’s official history. To boost performance, researchers developed magnetic core memory and bolted it on to Whirlwind. Magnetic core memory became the industry standard for the next 20 years.

SAGE also utilized primitive modems—the skeletal structure of cyberspace. Scientists at the Air Force Cambridge Research Lab in Cambridge, Mass., also figured out how to convert analog radar into digital code and transmit over a dedicated telephone line. This was one of the earliest workable modems.

Airmen also got their first taste of working in a computer-driven, interactive environment linking sites all over the country. This was an important early step in building up the cyberspace domain. “The primary responsibility for humans in the SAGE system would be their interaction with computers through the use of keyboards and other devices in order to specify which of the airplanes picked up and followed by radar and shown on the computer cathode-ray monitors should be targeted,” summarized Thomas P. Hughes in *Rescuing Prometheus,* his landmark book on innovation.

SAGE also stressed systems engineering skills because of the difficulty of developing and exploiting new computer and communications technology. In retrospect, "the military requirements for SAGE sytem placed it beyond the leading edge of software technology," noted a 1974 RAND report.

It took until 1958 for SAGE to become fully operational. By then, it was also obsolete. Still, SAGE marked the first major commitment of USAF dollars and expertise and provided components of the future cyberspace domain.

One of SAGE's flaws was its hierarchical communications design. What if a Soviet attack wiped out communications links and blinded SAGE and its successor air defense systems? Survivability of command and control in time of nuclear attack was a big preoccupation in the 1960s as the Soviet Union increased its bomber and missile forces.

A RAND Project Air Force researcher named Paul Baran took on the problem and ended up with another big push in the development of cyberspace—a theory of distributed communications.

Baran saw right away that accurate Soviet intercontinental ballistic missiles spelled big trouble for the current system.

"The proven development of the small [circular error probable] ICBM must evoke a major change of concepts of air defense," he wrote in a December 1960 report that was classified for decades. "Our communications systems are for the most part conceived upon the model of hierarchical networks. An entire network may be made inoperable at the cost of a few missiles cleverly directed against a few switching center targets."

What did a superbly hardened command center matter if the links to the air defense sectors and missile fields were destroyed?

The SAGE network was a case in point, according to Baran. Each hierarchical node fed a central control point. The central control points then retransmitted to a central station. Wiping out the key links would shut down command and control.

Instead, Baran envisioned a series of backup centers with commanders. As long as they all had good information, nearly any one of the senior military officers in charge of the set of centers could make a good decision on how to cope with incoming attacks. Baran described potential non-hierarchical network formats starting with a simple "round robin" network. The key was "distributed computation, or totally independent apparatus at each node" providing such routing "without reliance upon a vulnerable central computer."

In Baran's concept, the message would travel over the shortest path, carry a security tag, and have its geographical point of origin authenticated. The system as a whole would be set up to identify malfunctions right away. Baran's work on Strategic Air Command's nuclear command and control problem laid out a crucial turn in the roots of networking and the Internet to come.

Platform via ARPAnet

By the 1970s, much of the groundbreaking work in cyberspace was tucked under the Pentagon's Advanced Research Projects Agency. ARPAnet was not conceived as a military communications project. Instead, the main motivation was to facilitate time-sharing by linking together powerful computers that were geographically separated. Computers at major USAF research centers such as RAND and Lincoln Labs were on the net by April 1971.

ARPAnet connected only big computers hosted at universities and companies. The National Security Agency went off and built its own version of the ARPAnet called Platform.

For the Air Force, this had two cyber implications. Cyberspace would grow in deep secrecy at NSA as signals and intelligence analysis became closer entwined with the cyber world. Airmen would be closely involved in that work, too.

However, cyberspace would also grow from the worlds of education and business. With commercial companies producing faster, more capable computers, USAF turned its focus to tactical applications for information technology.

Air Force Systems Command commissioned a study in March 1971 titled "Information Processing/Data Automation Implications of Air Force Command and Control Requirements in the 1980s." Its purpose was to scope the information processing technology anticipated for command and control of Air Force combat units in the next decade.

Software was becoming the problem of the 1970s; USAF was already spending almost $1.25 billion per year on software—three times more than hardware spending for automatic data processing. And software progress was already attracting complaints. "Software has yet to live up to its potential in [command and control] systems," noted the 1974 RAND report.

However, heavy investment in software spread online systems throughout Air Force major commands. Systems such as the Strategic Air Command Automated Total Information (SATIN IV), the Military Airlift Command Informa-

USAF photo by TSgt. Cohen Young

Then-Secretary of the Air Force Michael Wynne announced in 2006 that USAF would create a cyberspace major command. USAF pulled back and made 24th Air Force the cyber component, under Air Force Space Command authority.

USAF photo by SSgt. Patrick Dixon

Airmen set up a satellite dish in 2009 at Aviano AB, Italy.

tion Management System (MACIMS) scheduler, and others were "online to dozens or hundreds of interactive users, processing several jobs or transactions simultaneously."

By the 1970s, USAF was also routinely exploiting the online environment for data management and display. In the future, the Air Force planned to extend real-time scenarios and online command decision aids. Based on the use of ARPAnet, Air Force leadership also concluded that real-time digital communications processing would be fully available to the Air Force of the 1980s.

With the advent of the 1980s, USAF completed the shift from technology innovator to customer. In early 1982, the Air Staff looked at the growth of information technology and concluded that the Air Force was no longer a leader in this area, per a study prepared for Chief of Staff Gen. Charles A. Gabriel.

Nor was USAF footing the development bill. Commercial hardware and software dominated—and would lead to new problems.

For the moment, it was the fastest path to changing the information environment for airmen. The 1980s marked a period when the user became a communicator, as one Air Force history put it. Gone were the days of limited access to computers and networked systems. The 1980s brought desktop applications to Air Force offices and command posts. Military nodes on the ARPAnet expanded, as did local area networks.

Tactics and exploitation of the information domain were about to become big challenges. The late 1980s demonstrated to all the inherent vulnerability in the medium.

In 1986 a hacker from West Germany named Markus Hess carried out a much more cautious and deliberate program of espionage. The Air Force was also involved, via agent Jim Christy of the Office of Special Investigations.

The case began when a systems administrator in California named Clifford Stoll was asked to investigate a tiny unpaid bill of 75 cents—an anomaly in the Lawrence Berkeley Laboratory system. For Stoll, that anomaly began a trail that led ultimately to Hess, who was conducting computer espionage for the KGB.

"The intruder was impressively persistent and patient," observed Stoll in his 1988 article, "The Wily Hacker," Hess attempted to hack 450 different systems. To enter the computers, he exploited weaknesses such as a program called GNU Emacs that allowed mail users system administrator privileges under certain conditions. Hess then searched root directories for files with words like nuclear, SDI, NORAD, or KH-11, one of a family of high-resolution clandestine satellites.

Stoll started a log of the hacker's activity and kept online to trace him. Soon he was sure the hacker was spying.

"With thousands of military computers attached, the MILNet [an early network] might seem inviting," Stoll conjectured. No classified computers were connected to the net, but there were treasures to be had, such as access to abstracts of nuclear, biological, and chemical warfare plans pertaining to Europe.

Now Stoll had to get someone to take seriously his report of a wily intruder on the loose. One of the first to encourage him was Christy.

The office was already handling computer crime, and Christy immediately understood the need to let the hacker keep operating as he electronically waltzed from Army computers to the White Sands Missile Range, N.M., to Ramstein AB, West Germany. Tracking Hess was one of the earliest efforts at data forensics—soon to become an essential tool of operations in cyberspace. In fact, Air Force OSI was later designated executive agent for Pentagon cyber crime and forensics.

The Hess case crystallized with a telephone trace. It turned out Hess was accessing US sites through a West

USAF photo by A1C Kate Thornton

A1C Corey Frey disassembles a computer tower at Ellsworth AFB, S.D. Client systems technicians such as Frey provide account support and troubleshoot computer problems for on-base clients.

German telecom provider. Stoll and the FBI created dummy files to entice Hess to linger long enough for a definitive phone trace. It worked.

Hess spent an hour perusing one set of files and was traced to the University of Bremen in West Germany. He was later convicted of spying for the KGB by the German authorities, who put Hess and his accomplices on trial in 1990. They received sentences of up to two years and, later, probation.

Then, on Nov. 2, 1988, 23-year-old Robert T. Morris placed a self-replicating worm on the Internet designed to multiply and seek out other hosts. The Morris worm overtasked computers, by one estimate crashing 6,000 of the 60,000 Internet hosts. DARPA formed its first computer emergency response team (CERT) during the Morris incident.

By the 1990s, the targets for cyber war were changing. Desktop machines, email, online connections, and Internet browsers surpassed the architecture of the 1980s and brought unprecedented access to data. Linked systems with many portals presented fruitful targets for attack.

Hack Attacks

For the Air Force, computer network defense became an essential for theater warfare. In the lead was the 609th Information Warfare Squadron established by Lt. Gen. John P. Jumper at 9th Air Force in 1995. This was the first effort to "conceive, develop, and field IW [information warfare] combat capabilities in support of a numbered air force," noted the unit's history.

The Air Force in the 1990s opted for the term "information warfare" to signify a greater mission than the operations of computers, networks, and routers. Information warfare carried the full set of cyber missions and activities, to include reconnaissance, defensive operations, offense, and exploitation. The 609th was "the first of its kind designed to counter the increasing threat to Air Force information systems," read its initial tasking.

"It was a combination of past warfighters, J-3 types, a lot of communications people, and a smattering of intelligence and planning people," said now-retired Col. Walter Rhoads, the first commander of the unit. The 609th made its mark during a Blue Flag exercise in 1996. "We had control of the Blue Force air tasking order," he recalled.

Rhoads estimated the 609th spent 70 percent of its time on offensive operations. The other 30 percent was defending networks by blocking hostile IP addresses and taking other actions. Eventually, the mission of the 609th extended to defending networks in the US Central Command area of responsibility. The initial split of offensive and defensive operations was mirrored at the national level with the task forces of the Defense Information Systems Agency or DISA.

USAF photo by William Belcher

Cyber airmen work at the 624th Operations Center at Joint Base San Antonio-Lackland in Texas. The 624th is part of 24th Air Force, USAF's cyber component.

The 609th IWS faced a major test in February 1998. Hackers launched a month-long offensive against DOD networks and Air Force and Navy bases, but no breaches occurred at installations defended by the 609th.

By 1999, the information warfare mission had grown so big that USAF moved the 609th mission into the larger Air Intelligence Agency. Detachments from the 609th would help defend numbered air forces.

At the turn of the century, cyberspace gained national prominence during the Y2K drama. The White House announced a new national cyber security strategy in February 2003, as well, and by the mid-2000s, US Strategic Command had gained a wider global role, which included responsibility for computer network defense and offense under its mission set.

But was USAF's late 1990s decision to tie cyber to the air operations centers and to the larger intelligence apparatus still sufficient in the 21st century? Not quite, senior leaders concluded. With a solid foundation already in place, the Air Force moved to embrace the cyber domain as a formal part of its mission.

In 2005, Secretary of the Air Force Michael W. Wynne listed cyberspace operations as one of the "sovereign options" provided by USAF for the nation.

Wynne followed up in November 2006 by designating 8th Air Force as the command responsible for cyber operations. But USAF pulled back, canceling the proposed stand-up of a service cyber command in 2008. Later, the Air Force created 24th Air Force as its cyber component and placed it under Air Force Space Command's authority.

For the Air Force, now the question remains how much the service should invest in creating cyber capabilities for use in the joint environment, especially as sequestration pressures mount.

"The US Air Force has a longer, more distinguished heritage in the cyber domain than any other military in the world," wrote Healey.

Airmen will be expected to deliver their best in the cyber realm, and history suggests requirements will change—and change fast. Cyberspace is a domain that rewards the proactive.

Perhaps the old motto of the 609th Information Warfare Squadron says it best—Anticipate or Perish. ■

Rebecca Grant is president of IRIS Independent Research. Her most recent article for Air Force Magazine *was "The Rover" in the August issue.*