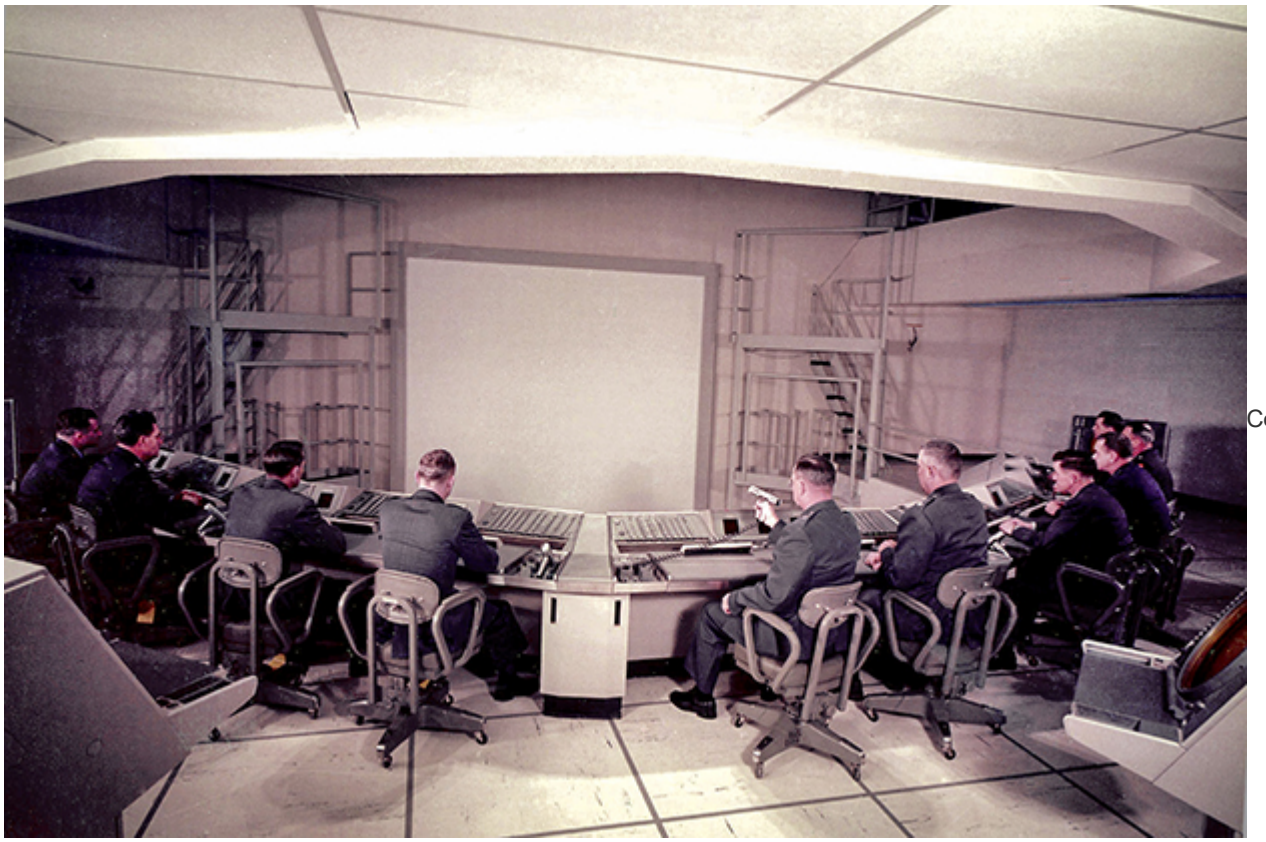
Air Force Magazine

From Cybernetics to Cyberspace

JANUARY 2019
JASON HEALEY

The roots of digital warfare date back to the birth of the US Air Force.



Command post staff use computers at a SAGE Combat Center at Hancock Field, N.Y., to communicate with other SAGE sectors, monitor an air battle, and direct weapons in 1959. **Photo: USAF/MITRE Corp.**

Cyberspace may seem new and exciting, but the Air Force has been advancing cyber concepts, technologies, and operations for more than 70 years—since 1947, in fact, the same year the Air Force was established as a separate service.

"Cyber" today has become shorthand for all things digital, but the term was actually coined just after World War II as "cybernetics," the study of feedback, communication, and control. The term was derived from the Greek word for "steersman," which refers "to the fact that

the steering engines of a ship are indeed one of the earliest and best developed forms of feed-back mechanism," according to Norbert Weiner, author of Cybernetics. Despite the nautical reference, modern cybernetics began with a wartime air-defense problem: How to better aim anti-aircraft guns at fast-moving targets flown by pilots keen to avoid getting hit.

Before World War II, the US Army had basic air-defense radars and fire-control directors that required up to nine operators. It was clear during the Battle of Britain that targeting fast-moving bombers required faster, automated solutions. The Tizard Mission to share research and development secrets between the United States and United Kingdom led to a crucial breakthrough—a "gun-laying" radar to guide servo-driven, anti-aircraft guns firing shells with proximity fuses. This automation both improved accuracy and reduced the number of soldiers needed.

But even radar-guided guns could only aim at spots where planes were likely to be based on their previous path and altitude. Could a system predict enemy pilots' evasive tactics and point the guns accordingly? Weiner, an MIT scientist, spent his war years working on this problem, mostly unsuccessfully.

While his research did little to help Army gunners, the processes of feedback, communication, and control that he developed led him to create the new science of cybernetics.

Cyber warfare specialists with the 175th Cyberspace Operations Group train at Warfield ANGB, Md., in 2017. **Photo: J.M. Eddins Jr./USAF**

THE AUTOMATED AIR FORCE

The progression from World War to Cold War accelerated the development of cybernetic concepts. The newly created Air Force was at the center of it all, especially for the critical problem of automating air defense. Since the Battle of Britain, the areas to be monitored had grown, the aircraft were far faster, and the bombs more devastating. Any solution would have to be scaled up to intercept Soviet bombers before they reached the homeland, making automation through cybernetics the only plausible response. Thus was born the Semi-Automatic Ground Environment (SAGE) system, the world's first computer network.

In 1950, the Air Defense Systems Committee drew on Weiner's ideas of feedback, communication, and control to design and build a series of networked radar stations feeding powerful computers. By 1954, SAGE was complete, with a continental network of radar stations, nearly two dozen supercomputers the size of buildings and hundreds of field sites, all connected by telephone lines. SAGE's software programmers at Lincoln Laboratories (located at then-Hanscom Field, Mass.,) had to learn to write binary code through trial and error, and invented concepts such as assembler programs, that have since become central to programming. In 1960, J.C.R. Licklider, a member of

SAGE working on human factors, wrote an Air Force-funded essay about this emerging “Man-Computer Symbiosis” with insights still relevant today. Humans “will set the goals, formulate the hypotheses, determine the criteria, and perform the evaluations. Computing machines will do the routine work that must be done to prepare the way for insights and decisions,” he said. In the early 1960s, SAGE became the Ballistic Missile Early Warning System (BMEWS), tracking missiles as efficiently as SAGE had identified bombers.

It was natural for the Air Force to take the lead in these early computer networks. The next cybernetic developments—sensory feedback and virtual reality—may not seem as close a fit for airmen. In 1955, the Air Force was experimenting with prototype nuclear-powered jet engines for a new generation of bombers that could stay aloft for weeks at a time. The maintainers needed to handle the radioactive fuel while shielded, a task requiring superhuman strength and delicacy. This led to the development of the “Handyman,” an exoskeleton suit with powerful mechanical arms that provided sensory feedback. The underlying technology is now used in everything from power steering and fly-by-wire systems to video-game controllers. Few know that Air Force labs pioneered it.

In the 1970s, such revolutionary human-to-machine and machine-to-human interaction, combined with the declining costs of computing power, drove Air Force cybernetic research into virtual reality (VR). After the Vietnam War, the Air Force’s aging fleet was due for a refresh, and the service’s leadership saw the potential for major gains from a cockpit that could display far more information—about the aircraft, environment, friendlies, and hostiles—without overloading the pilot. Rather than focusing on just a physical redesign, the Air Force “virtualized” this information into the Visually Coupled Airborne Systems Simulator (VCASS) helmet. While cutting edge, these helmets were unwieldy, even at normal Gs. Fortunately, the technology had other applications, such as increasingly realistic flight simulators and heads-up displays. Today, helmet-mounted displays for fifth generation fighters allow the pilot to “look through” the airframe, and VR technology is finally coming of age to deliver aerial supremacy.

By the mid-1980s, the possibilities of this virtual world had captured the public’s imagination, and this Air Force-driven view of the modern era—along with the new science fiction of writers like Vernor Vinge and William Gibson—led to the modern concept of “cyberspace” as a computer-generated dimension distinct, yet, interconnected with the physical world.

Hindsight reveals the divergence of two distinct “cyber” tracks in the Air Force. The first was closely tied to Wiener’s 1947 original cybernetic concepts around guided anti-aircraft fire. The Air Force would come to call this track “information in war,” encompassing information operations, command and control, electronic warfare, and new classes of precision weaponry. Retired Air Force fighter pilot Col. John R. Boyd combined these ideas from the 1970s to the 1990s with his OODA Loop: to Observe, Orient, Decide, and Act to “unravel the competition.”

The second track was rooted more firmly in the new “cyberspace” of increasingly ubiquitous computers and the global networks linking them into a unified, borderless whole. That track would lead to “information warfare,” a truly novel kind of warfare in which information would be both weapon and target.

Airmen compete in a cyber weapons competition in San Antonio, Texas. In the 1990s, USAF created the first unit anywhere to combine offensive and defensive cyber operations in direct support of a warfighting commander. **Photo: USAF/TSgt. R.J. Biermann**

THE AIR FORCE IN CYBERSPACE

Lt. Col. Roger R. Schell drew on his experiences with BMEWS and SAGE to "red team" computer networks in the 1970s. "Computers are at the heart of" new Air Force capabilities like dynamically retargeting ballistic missiles, he wrote in 1979, so if those computers "were penetrated, an enemy could retarget the missiles to impact on low-value or even friendly targets as part of a surprise attack!" It wasn't long before the first cyber conflict emerged.

In 1986, German hackers stole unclassified information about the Strategic Defense Initiative (President Ronald Reagan's "Star Wars") and sold them to the Soviet KGB, a case in which the Air Force Office of Special Investigations played a leading role. Just two years after that, an automated worm took down 10 percent of the early Internet, spurring the Air Force to create a cyber response capability years ahead of the other services. The Air Force Computer Emergency Response Team (AFCERT) at then-Kelly AFB, Texas, reported to the Electronic Security Command (later the Air Intelligence Agency and now 25th Air Force).

While these incidents were important, they remained far from the service's main warfighting concerns. During Operation Desert Shield, the buildup of US and coalition forces to eject Saddam Hussein's Iraqi divisions from Kuwait, the Defense Department suffered an early shock: Dutch anti-war hackers penetrated 34 DOD computer systems, which had "easily guessed passwords [and] well-known security holes in computer operating systems," according to a lessons-learned report. The hackers accessed systems with information on logistics, weapon systems, and personnel, causing concern that they might have been able to disrupt the massive flow of forces to the theater.

In September 1993, the Air Force restructured its Electronic Warfare Center to create the Air Force Information Warfare Center (the AFIWC, now the 688th Cyberspace Wing of 24th Air Force), aiming to drive change in the service for both information in war and information warfare. The Government Accountability Office reported in the mid-1990s that "because the Air Force's computer emergency response team resources are larger and more experienced" as a result of confronting these earlier events, "they have had better success in detecting and reacting to attacks than either the Navy or Army."

In 1995, then-Air Force Secretary Sheila E. Widnall and Chief of Staff Gen. Ron R. Fogleman cosigned a revolutionary document, the Cornerstones of Information Warfare, which included a passage that even now remains a compelling description for why cyber is indeed a new domain of warfare:
Before the Wright brothers—air—while it obviously existed, was not a realm suitable for practical, widespread military operations. Similarly,

information existed before the Information Age. But the Information Age changed the information realm's characteristics so that widespread military operations within it became practical.

Soon after, in a second major effort, the Air Force created the 609th Information Warfare Squadron at Shaw AFB, S.C. The 609th, in support of Air Forces Central Command, was the first unit anywhere to combine offensive and defensive cyber operations in direct support of a combat commander. Its first commander, then-Lt Col. Walter E. Rhoads, a former F-117 pilot, built up a team of airmen to plow a fresh path in cyberspace but, as "nobody knew what a 'cyber warrior' was," the unit was built from "a combination of past warfighters, J-3 types, a lot of communications people, and a smattering of intelligence and planning people." The unit had early successes getting senior officers to even realize what information warfare was and that "it was actually a viable capability." In one exercise, the 609th proved its mettle by seizing the blue force Air Tasking Order: "They gave us a two-hour window to play in, and we got it within two hours."

The lessons from these operations were critical to an exercise that would shake policymakers at the Pentagon and White House in 1997, when "red team" hackers from the National Security Agency (NSA) participated in a Joint Staff exercise, Eligible Receiver. Attempting to access and disrupt American networks and infrastructure, the NSA red team had little difficulty.

This key exercise exposed a generation of political, military, and intelligence leaders to the dynamics and potential impact of cyber operations.

In 1998, with these lessons still fresh, technicians at the AFCERT detected cyber intrusions into multiple bases. Some of the attacks seemed to trace to Iraq just as the US military was flowing forces into the Middle East to dissuade Hussein from evicting nuclear inspectors. Deputy Secretary of Defense John Hamre briefed President Bill Clinton that this attack, dubbed Solar Sunrise, relaying that it might be the beginning of a cyber war as presaged by Eligible Receiver, only a few months earlier. As it turned out, the intrusions were serious—but the connection to Iraq was a false alarm. The intruders turned out to be teenagers spurred by a mentor to poke into DOD systems for fun. In the aftermath, the Washington Post asked a question still echoed today, "Why hadn't the military bothered to effectively patch known vulnerabilities?" Worse, the Pentagon worried, if children can scare us to the core, what could determined professionals do?

To better answer these questions and speed defensive responses, the Joint Task Force for Computer Network Defense (JTF-CND) was established in December 1998, and AFCERT was immediately attached to the unit as its Air Force component. Air Force Maj. Gen. John H. Campbell, a former F-16 and F-15 pilot, won the coveted role of running the world's first joint cyber command.

Cyber seemed like such a natural fit for the Air Force that in 2007, Lani Kass, director of the Air Force's Cyberspace Task Force, announced that "cyber delivers on the original promise of airpower." It was fast-changing and very high tech, offense had the advantage over defense, and cyber attacks with their rapid and intercontinental reach could bypass an enemy's fielded forces. Air Force doctrine from 2010 highlighted these similarities between aerospace and cyber power, emphasizing that airmen should be in charge.

Airmen normally think of the application of force from a functional, rather than geographical, perspective [and according to AF basic doctrine, AFDD-1] "airmen conduct a greater percentage of operations not just over the horizon but globally, expanding operations first through space and now also in cyberspace." … Thus, cyberspace operations should be tightly integrated with capabilities of the air and space domains into a cohesive whole, commanded by an airman who takes a broader view of war, and unconstrained by geographic boundaries.

Then-Lt. Col. Gregory J. Rattray wrote the first ever cyber warfare Ph.D. in a 1997 dissertation—later to be published as Strategic Warfare in Cyberspace—which made an extended comparison of the promises made by early airpower enthusiasts and the nearly identical ones made (then and now) by early cyber enthusiasts. In 2011, the service also produced arguably the world's first true "cyber" general, Brig. Gen. (now Lt. Gen.) Bradford J. Shwedo, who had predominantly been in cyber (as opposed to communications or intelligence) jobs since he was a young captain. Lt. Gen. John D. Bansemer earned his cyber chops as a captain of an elite NSA hacking program starting in 1996 and became the first cyber three-star officer 17 years later. Both Rattray and Bansemer went on to oversee military cyber operations at the National Security Council in a position the Air Force had a lock on for most of the 2000s.

Unfortunately, Air Force efforts in cyber leadership subsequently stalled because of mission confusion within the Air Force, rivalry within DOD, and the growing strength of the other services in the field.

Secretary of the Air Force Sheila Widnall saw the importance of cyber to the emerging USAF mission. **Photo: USAF**

STEPS BACKWARD AND FORWARD

Constant shifts in focus undermined the service's early momentum in cyber. Because nearly every aerospace mission depends on or could influence cyberspace, airmen from intelligence, electronic warfare, warfighting, space control, and computers and networks all saw cyber as a natural extension of their own areas of expertise. Each community pressed the case to "normalize" Air Force cyber with its specialty in charge.

In the 1990s, the Air Force viewed cyber as a subset of information warfare, with the emphasis on warfare. Many of the first cyber missions resided with the intelligence specialists at the Air Intelligence Agency (AIA) who "defended the information highway" with unique skills and tools, "participating in, rather than just supporting, combat operations." To normalize the mission, the AIA was put under Air Combat Command in 2001 to recognize "the growing role of information operations as a warfighting weapon" and more seamlessly integrate cyber with targeting, electronic warfare, and traditional warfighting processes and missions. In parallel, at the Air Staff, the Intelligence directorate (now A2) folded under Operations (A3) to better organize all aspects of information operations.

ACC remained the Air Force's cyber lead for eight years until 2009, when the mission was transferred to Air Force Space Command under the logic that cyberspace—it was felt—depends on space-based satellites, and both "space and cyberspace forces are inherently global … unfettered by time and distance." Then, in 2018, that decision was reversed, with the cyber and intelligence missions (the 24th and 25th Air Forces) reassigned back to ACC.

"Normal" again meant integrating the cyber mission with electronic warfare and other traditional Air Force combat tasks. One senior Air Force general boasted that "cyber operations and intelligence in cyber capabilities under one command is a significant step toward enhancing our warfighting capabilities," perhaps not realizing the "significant step" was merely a return to a prior command relationship.

Meanwhile, the other services (as well as the National Security Agency) began to worry the Air Force was seizing the cyber missions for itself. To some degree, this was true. Much of the early defensive, investigative, and offensive capability was blue-suited, and the early "cyber power enthusiasts" were the Air Force generals who ran the NSA from 1996 to 2005, Lt. Gen. Kenneth A. Minihan and then-Lt. Gen. Michael V. Hayden.

The perception in the rest of DOD that the Air Force intended to grab the entire cyber mission tipped toward outrage after the service updated its mission statement in December 2005: "… to fly and fight in the Air, Space, and Cyberspace," and then, soon after, announced a provisional Air Force Cyber Command, built on the 8th Air Force. This command projected the somewhat grandiose goal of being "the

provider of [cyber] forces that the president, combatant commanders, and the American people can rely on," prompting the rest of the defense establishment to block what they saw as a unilateral Air Force power grab. In response, Chief of Staff Gen. Norton A. Schwartz shelved the plans for the new command, instead organizing cyber airmen as the 24th Air Force. But the damage was done. It is probably not a coincidence that no Air Force officer has run the NSA (or US Cyber Command) since 2005, the longest drought for any service since the NSA's creation in 1952.

Another reason the Air Force lead faltered was simply that the other services caught up, especially after the creation of US Cyber Command in 2010. This resulted in stronger and more centralized leadership from DOD while the other services steadily built their own cyber capabilities (run by three-star flag officers, while Air Force efforts are still run by a two-star). These factors reduced the scope for a particularly blue-suit cyber identity. Few cyber missions, other than defeating integrated air defenses, seem specifically related to the service's doctrinal missions. Strategic attack, for example, was the justification for a separate Air Force in the first place. But if sailors and soldiers can cause similar strategic effects using similar cyber capabilities to those of an airman, it was natural to ask, "what sets airmen apart in cyber operations?"

CYBER-MINDEDNESS

Of course, it turns out that decades of history set the Air Force apart. It has been two decades since airmen first started learning the lessons of cyber conflict at the 609th Information Warfare Squadron, six decades since the automated air defenses of SAGE, and seven decades since Norbert Weiner first coined the concept of cybernetics from his work on the anti-aircraft problem. But little of this history is remembered.

The cyber challenges over the horizon in 2028 and 2038 might be shattering if America's Air Force is not prepared. The response to the interactions between four trends, in particular, will determine success: the recombination of "cyber" and "information" warfare; overwhelming societal dependence on information technology; artificial intelligence; and the return of great power competition raising the risk of major war.

The Air Force should build on its early cybernetics history to play a lead role in the future of cyber. As America's adversaries seek to lock out US aircraft and ships by means of advanced area-denial defenses, the Air Force should leverage its inherent strengths to suppress these defenses, including cyber means and other capabilities to cause strategic effects without the need to penetrate conventional defenses. The nation created the Air Force in 1947 to have a force specialized in rapidly bypassing the enemies' fielded forces with new, technological capabilities. This new battlefield of cyberspace should be a natural fit for airmen.

The exact future is uncertain, but this much is clear: A mentality of "cyber-mindedness" will be just as crucial in the future as that of "air-mindedness" has been since the advent of flight—an understanding which can only be achieved by studying and building on the legacy of the Air Force's cyber history. This heritage must be taught in our professional military education, especially Squadron Officer School. Just as officers and cadets must learn about the service's heroes in air and space, they should also know of Air Force cyber pioneers: Rattray, Rhoads, Campbell, and Hayden.

The Air Force led cyber before it was cool, before even the invention of the computer or the Internet. Peek behind nearly every critical cyber technology and you'll find blue-suiters. Today's airmen should internalize this heritage and renew our dedication to driving the future of cyberspace.

—

Jason Healey is a senior research scholar at Columbia University's School of International and Public Affairs and author of the first history of cyber conflict, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. He is a 1991 graduate of the US Air Force Academy. This is his first article for *Air Force Magazine*.