Claiming the Lost Cyber Heritage

The Air Force ensures that newer generations of Airmen learn through the vicarious experiences of those who have gone before them. They are taught to admire Eddie Rickenbacker and Billy Mitchell, and cadets and officers are tested to ensure they understand the lessons from Big Week, MiG Alley, and Rolling Thunder to Iraqi Freedom. Understanding this history and heritage is the primary way to turn the vicarious experiences of past generations into cumulative knowledge to educate Airmen of the future. According to the official Air Force website, heritage is "dedicated to the former Airmen who developed the independent Air Force and continue its evolution into cyberspace. . . . The people, events and equipment of the past are integral to understanding the future."[1] Yet there is a particular heritage that has been forgotten and ignored as irrelevant. A recent search for "cyber" on official historical sites of the Air Force led to only four documents, no images, and a single video from 2012.[2]

Indeed, a fighter pilot that had never heard of the "hat in the ring"—who in fact spurned the history of airpower—would be an outcast. Yet this is not far from how the Air Force, and indeed the entire Department of Defense, treats the history of cyber conflict. Few, if any, Airmen involved in cyber operations today are likely to remember the major cyber conflicts, pioneering cyber leaders, doctrine, or units of the past.

How many of today's Air Force cyber warriors know they can trace their lineage to AF cyber operations in the mid 1980s? Nearly 25 years ago a lone special agent in the Office of Special Investigations was intrigued by a call from an astronomer turned system administrator who found intruders in his networks at a national laboratory. The Air Force helped unravel an international espionage ring, nicknamed the Cuckoo's Egg, where German hackers sought classified material on the Strategic Defense Initiative, which they sold to the Soviet KGB. Special Agent Jim Christy, the first cyber "ace," is now retired but still delivering for the Air Force at the Defense Cyber Crime Center.

How many of today's Air Force cyber warriors know when the Air Force declared cyberspace a new domain for military operations? The answer is not 2011 when the Department of Defense declared that the military would "treat cyberspace as an operational domain," nor even in 2005 when the Air Force added cyberspace to its mission statement as a domain in which to "fly, fight, and win," but a decade earlier. In 1995 the secretary and chief of staff jointly signed the Foundations of Information Warfare which laid out basic definitions and principals for how the Air Force would work in cyberspace.

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 operations became practical.[3] This statement is at least as good as anything written since by any military anywhere.

How many of today's Air Force cyber warriors have even heard of the world's first combat cyber unit? In 1996, the Air Force established the 609th Information Warfare Squadron (motto: "Anticipate or Perish") at Shaw AFB to support CENTAF with combined offensive and defensive cyber missions "to fully operationalize information warfare on behalf of the JFACC [joint force air component commander] and the fighting forces."[4] This unit, the first such unit in the Air Force, is likely the first anywhere in the US military and the world.[5] The unit invented the first INFOCON, now a standard defensive alert condition. It exercised heavily with CENTAF and "had control of the blue force air tasking order. They gave us a two-hour window to play in, and we got it within two hours," according to the unit's commander, then-lieutenant colonel Walter "Dusty" Rhoads, another Air Force cyber pioneer who had roles in every major joint cyber war-fighting organization for the next 10 years.[6]

These efforts at the 609th were just one part of using cyber to support the war fighter. As Maj Gen John Casciano, then head of AF intelligence put it in 1996,

> Anything we do in the Air Force has to be consistent with a . . . JTF commander's requirements and must meet those objectives. We believe that IW is absolutely critical and integral to Air Force operations at the JFACC level and below. We have some things to offer other communities, but our focus is on the operational and tactical levels of warfare. A lot of the targets and a lot of the things we would want to affect—command and control nodes and the adversary's integrated air defense system (IADS)—are things the Air Force worries about on the battlefield.

How many of today's Air Force cyber warriors know the first joint cyber commander was from the Air Force? It was not GEN Keith Alexander, USA, who took charge of US Cyber Command in 2010, but Maj Gen John "Soup" Campbell, USAF, the founding commander of the Joint Task

Force–Computer Network Defense in 1998. His approach to cyber operations was rooted deeply in his Air Force identity, "I grew up as a fighter pilot. My job was to blow things up, make smoking holes . . . so I always took it in that direction."[7]

These are not empty facts or trivia for cyber operators to play on a long nightshift.[8] They are emblematic of the rich heritage of the Air Force in cyberspace and illustrate the importance of learning the lessons of history. The Air Force is not responsible for all the problems of the Department of Defense in cyberspace. But it can fix those that it controls. If the Air Force is going to become the premiere force to fly, fight, and win in cyberspace, it must reclaim its proud cyber heritage and build "cyber-mindedness," just as it has a tradition of air-mindedness. If it can succeed in this, the Air Force can again be seen as the cyber thought leaders in the military service and show the way for the other services, the Department of Defense, and the intelligence community. If not, the service is likely to continue to relearn old lessons and struggle under misperceptions with little relation to past experience.

Over two decades, the Air Force, and the Department of Defense in general, have made little progress on important policy and operational issues, but few realize just how little progress because few know how far back the story goes. For example, the sentiment behind the next two paragraphs should be familiar to many of today's AF cyber professionals:

> Nobody knew what a "cyber warrior" was by definition. It was a combination of past war fighters, J-3 types, a lot of communications people and a smattering of intelligence and planning people. . . .
>
> The unfortunate part . . . was that the offensive side was still classified. You couldn't even discuss it in an open forum. . . . But behind the scenes [we were] getting it integrated into the war fighters' mentality, understanding the air tasking orders. . . . [We were] an Air Force unit and we had to understand how to get cyber introduced into the thinking of the commanders.

Unfortunately these quotes resemble those of today, but they are actually from Rhoads speaking about the 609th IWS in 1995. Likewise, consider the following quotes. One is from Rhoads, circa 1996, the other from Maj Gen Richard Webber of Twenty-fourth Air Force in 2009. *Why can't we even tell the difference*?

> I liken it to the very first aero squadron when they started with biplanes. We're at the threshold of a new era. . . . We are not exactly sure how combat in this new dimension of cyberspace will unfold. We only know that we are the beginning.[9]

> I almost feel like it's the early days of flight with the Wright Brothers. First of all you need to kind of figure out that domain, and how are we going to operate and maintain within that domain. So I think it will take a period of time and it's going to be growing.[10]

American Airmen learned how to dominate the aerial domain and deliver integrated combat effects in just 15 years between the first flight of the Wright Brothers and the Battle of Saint-Mihiel. Yet in the same amount of time since the first AF combat cyber unit, we have made so little progress in the cyber domain that quotes from key commanders a decade apart are indistinguishable.

This blindness to history has immediate operational implications. Much of what is treated as received wisdom is in fact not rooted at all in the history of cyber conflicts. Many of today's cyber warriors will tell you with all confidence that (1) cyber conflict is new and ever changing, (2) massive surprise attacks can easily prostrate nations, and (3) everything that is important happens at the speed of light. In fact, a study of cyber conflict history by the Atlantic Council and the Cyber Conflict Studies Association has shown that all three of these are incorrect or misleading.

There has been no essential discontinuity between cyber conflicts of 20 years ago and those of today. Of course, there are differences: adversaries have become more capable, underlying technologies (offensive and defensive) have changed, and corporations are now feeling the brunt of major espionage attacks. Yet, despite these developments, the dynamics of today's conflict would be familiar to the Airmen that fought them at the 609th Information Warfare Squadron in 1995.

Likewise, disruptive cyber attacks have so far tended to have effects that are either widespread but fleeting or persistent but narrowly focused. Few, if any, attacks so far have been both widespread and persistent. As with airpower, cyber attacks can easily take down many targets, but keeping many down over time has so far been out of the range of all but the most dangerous adversaries.[11]

And strategically meaningful cyber conflicts rarely occur at the "speed of light" or at "network speed." True, individual tactical engagements can happen as quickly as our adversaries can click the Enter key, but cyber conflicts, such as Estonia, Georgia, Stuxnet, and the Conficker worm, are campaigns that take weeks, months, or even years of hostile contact between adversaries.

At least once before, the Air Force suffered similar "doctrinal lock in," ignoring the emerging lessons from experiences in a new domain. In the 1930s, as all Airmen know, bomber enthusiasts preached that "the bomber would always get through," across international borders and distances, and that hitting 154 known targets would quickly knock Germany out of the fight in six months.[12] Their exercises reflected this view, which left them completely unprepared for the lengthy attrition battles of World War II. The Army Air Corps lost nearly 10,000 bombers and took years to achieve strategic effects, having entered the war lacking appropriate doctrine, defensive firepower, and intelligence for targeting and bomb damage assessment.

Airmen learned that finding the right target for strategic effect is difficult, and there is a tremendous difference between temporarily disabling a target and permanently destroying it. Even with strategic attack in its DNA and a decades-long history of cyber conflict, the Air Force is still not recognizing the right lessons, much less learning them. It should be natural for the Air Force to realize that the "speed of light" of cyber operations is deceptive. There is no reason why Airmen should be fooled on this point, because they understand even though a dogfight can be over before the losing pilot even knows it has begun, an air campaign is rarely decided by a single tactical engagement.

By thinking only of conflict at the speed of light, the Air Force will overinvest in capabilities and doctrine to automatically counterattack and will be unprepared for the long cyber campaign most of our adversaries seem to expect and appreciate. If speed is mistakenly seen as the most important factor, then rules of engagement will allow ever lower levels to shoot back without seeking authorization—a relaxation of the rules, which may not be in the long-term economic or military interest of the United States. The Air Force will continue to dogfight blindly, flying from tactical engagement to tactical engagement without having thought about tomorrow's battle or the one a year from now.

Similarly, Airmen should be the first to doubt it will be easy to have a prolonged strategic effect, even in cyberspace. If Flying Fortresses and Lancasters had difficulty achieving a strategic effect after dropping millions of tons of high explosives, we should never believe the fallacy that a few young hackers might take down the United States from their basement. This might be true in the movies or an espionage novel, but not in real life.

Yet basement-originated strategic warfare is a common theme from some who feel deterrence is difficult, since "cyberspace is fundamentally different. For someone with the right brainpower and the right cyber abilities, a cheap laptop and Internet connection is all it takes to be a major player in the domain."[13] These tools might help an adversary steal data or identities—even conduct a major intrusion like Solar Sunrise—but they are not sufficient to create a strategic effect requiring Air Force deterrent power.

This has been well known by Airmen since at least 1998 when Maj Gregory Rattray wrote his doctoral thesis, later published as *Strategic Warfare in Cyberspace*, with an extended comparison of how the early Army Air Corps struggles to learn how to fight in a new domain were directly comparable to what the Air Force was, and sadly still is, going through for cyberspace.[14]

These are all common misconceptions, but they are not supported by either the facts of cyber history or the experiences of Airmen. Perhaps soon, the world will see these kinds of attacks, but that is still no reason to ignore the past. By developing cyber-mindedness—a collective sense of the history, dynamics, possibilities, and limitations of cyber conflict—the Air Force can learn these and other critical lessons and prepare for the conflicts of the future.

The US Air Force has a longer, more distinguished heritage in the cyber domain than any other military in the world, but it is just one of the military services and should not be the *only* cyber service. As Major General Cascaino put it in 1996 when he ran the AF cyber units, "We don't claim [cyber] exclusively. We think we've got good ideas. We think we've got good capabilities. And we are reaching out to the other services and the joint community to offer what we have."[15] Fifteen years ago, this mindset helped the Air Force to be the world's preeminent cyber force, but not anymore. "For a brief period," as described by Lt Gen Bob Elder, retired, another AF cyber commander, "the AF was recognized as the thought leader on cyberspace, but when we narrowed our view, we undercut the basis for our leadership role."[16] Now retired, Major General Casciano echoes this sentiment, believing that "we have attempted to solve things organizationally and politically, not operationally."[17]

To reclaim this heritage, there are a number of entirely practical steps the Air Force must take.

- Commission the Air Force Historical Research Agency to conduct oral histories of the pioneers of the Air Force cyber mission and collect the official unit histories. This material should be the basis of a major study with appropriate lessons.

- Integrate cyber heritage and lessons into all professional military education (PME), starting with basic training and material for officer candidates (such as the Contrails guide) and continuing through all PME courses.

- Incorporate more detailed material on cyber heritage and lessons into classes such as Cyber 200 and 300 for the service's new cyber cadre.

- Encourage PME students to research and write on cyber heritage and lessons.

- Create a formal network to connect former AF cyber leaders, especially those retired or in the private sector. The Air Force created the earliest generation of cyber leaders, and many would enjoy the honor of being able to continue their association.

To further propagate this agenda, the Air Force Association—the main culture carrier for the service—is working with the Atlantic Council and the Cyber Conflict Studies Association to establish a distinguished panel of former AF leaders and cyber professionals to discuss other ways to build cyber mindedness and make the most of the service's cyber heritage. Some initiatives this group might consider may sound outlandish but are entirely reasonable if the Air Force indeed wants to establish itself as a force to "fly, fight, and win in air, space, and cyberspace." These include:

- How might AF units earn battle streamers for participation in major cyber conflicts? For example, the AF Computer Emergency Response Team played significant roles in Solar Sunrise, Moonlight Maze, and Buckshot Yankee. These conflicts may or may not be sufficiently intense to qualify for a streamer, but future conflicts might.

- What might be a cyber equivalent for missions flown, combat missions, and flying hours? These are all criteria Airmen use to understand the experiences of other Airmen. Defensive operators routinely block major attacks and respond to the adversary's changing tactics. Offensive operators intrude into adversary's systems. Each of these can be measured and rewarded and may have an equivalent in cyberspace, which can build cyber heritage and esprit de corps.

- What might be a cyber equivalent for aerial victories and qualification for becoming an ace? Cyber operators, both offensive and defensive, are in routine contact with adversaries looking to do America harm. Sometimes Air Force operators win and sometimes they lose, but the best among them win more consistently. A definition on what constitutes a victory, a concept which is sure to be very elusive, would be one way to celebrate the best traditions of Airmen everywhere.

Nearly 90 years ago, Maj Horace M. Hickam told a doubtful Morrow Board, "I am confident that no general thinks he can command the Navy, or no admiral thinks he can operate an army, but some of them think they can operate an air force."[18] Today, Airmen are sure they can operate a cyber force but have largely ignored the lessons from the history of cyber conflict and the service's own cyber heritage. The Air Force must start to inculcate cyber mindedness rooted in history and heritage.

The longer we think cyber conflict is new, the more we will repeat the same mistakes and relearn old lessons. Today's AF officers learn the Fokker scourge, daylight precision bombing, MiG Alley, and Rolling Thunder. So, must the new Air Force cyber cadre study *yesterday's* cyber operations to understand those of *tomorrow*? The call to today's Airmen, and especially the cyber cadre should be clear. Learn your history—know the units, understand the operations, and emulate the aces. And above all, incorporate the lessons. The Air Force used to know this and more. Once it reclaims this heritage, it can lead the world as the premiere force to fly, fight, and win in cyberspace.

Jason Healey
Director of Cyber Statecraft Initiative
Atlantic Council, Washington, DC

Notes

1. "Heritage," US Air Force official website, http://www.af.mil/information/heritage/index.asp.

2. Searches conducted on http://www.airforcehistory.af.mil/main/welcome.asp and http://www.afhra.af.mil/.

3. Gen Ronald R. Fogleman, USAF chief of staff, and Secretary of the Air Force Sheila E. Widnall, "Foreword, Cornerstones of Information Warfare," *C4I.org*, 1995, http://www.c4i.org/cornerstones.html.

4. Maj Gen John P. Casciano, comments to Air Force Association Symposia, 18 October 1996, http://www.afa.org/aef/pub/la9.asp.

5. The Air Force had created other cyber units—and was the first service to do so—such as the AF Computer Emergency Response Team and AF Information Warfare Center (AFIWC) in 1993. These critical units, however, did not directly support the war fighter in such a direct way with both offense and defense capabilities. Quote from Atlantic Council event convened by the author on 5 March 2012, "Lessons from Our Cyber Past: The First Military Cyber Units," http://www.acus.org/event/lessons-our-cyber-past-first-military-cyber-units.

6. Quote from Atlantic Council event convened by the author on 5 March 2012, "Lessons from Our Cyber Past: The First Military Cyber Units," http://www.acus.org/event/lessons-our-cyber-past-first-military-cyber-units.

7. Ibid.

8. Other important Air Force heritage that might have been include the first major cyber organization (AFIWC in 1993), that the first AFFOR cyber component was established in 1998 with Col Jim Massaro as AFFOR commander, and that the first real cyber general—that was in cyber jobs from his earliest days as a captain—is the current ACC/A-2, Brig Gen Bradford J. "BJ" Shwedo.

9. Lt Col Dusty Rhoads, "609 IWS: A Brief History, Oct 1995–Jun 1999," 1.

10. Maj Gen Richard Webber, Comments at 2009 Air Force National Symposium, http://www.afa.org/events/natlsymp/2009/scripts/091119-Webber.pdf.

11. This is most likely to change as nations put online more physical infrastructure, such as the Smart Grid.

12. Col Ed Crowder, USAF, "Pointblank: A Study in Strategic and National Security Decision Making," *Airpower Journal*, Spring 1992, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj92/spr92/crowd.htm, using information from the AWPD-1 plan for air war against Germany.

13. Gen William L. Shelton, remarks at Air Force Association, CyberFutures Conference and Technology Exposition, 22 March 2012, audio at http://www.afa.org/events/CyberFutures/2012/postCyber/default.asp (quote around 14:47).

14. See Greg Rattray, *Strategic Warfare in Cyberspace* (Boston: MIT Press, 2001).

15. Maj Gen John Casciano, comments at 1996 AFA Symposium.

16. Lt Gen Bob Elder, e-mail to the author, 24 May 2012.

17. Maj Gen John Casciano, e-mail to the author, 11 July 2012.

18. J. S. Shiner, *Foulois and the U.S. Army Air Corps: 1931–1935* (Washington: Office of Air Force History, 1983), 29.