# The Interim Years of Cyberspace

1st Lt Robert M. Lee, USAF

> *There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things.*
>
> —Machiavelli

Cyber power will be as revolutionary to warfare as airpower, but the current vectoring of the domain will determine which nation will hold cyber dominance and to what effect. In the early years of the cyberspace domain, the United States primarily considered cyber power a means of establishing broad command and control across the war-fighting domains. Cyberspace focused on communication; indeed, operational success depended upon maintaining the lines of communication. As the domain grew, it assumed additional roles to provide a support force to traditional military operations while experts explored other roles—a process that occurred at the highest levels of secrecy. Many of the first cyberspace leaders realized that cyber assets offered a number of options for attack, defense, and exploitation never

before afforded to military commanders. In a highly connected world where substantial advancements in technology were common, the capabilities and weapons in cyberspace became even more impressive.

The current stage of cyberspace development resembles the interim years between World War I and World War II, when airpower responded to challenges by emerging as a powerful military tool. No comparison does better justice to contemporary cyberspace than airpower during those foundational years. At that time, theorists and military officers, including Gen Giulio Douhet, Marshal of the Royal Air Force Hugh Trenchard, and Brig Gen William "Billy" Mitchell, helped guide the direction of airpower. As cyberspace reaches its full potential as a domain of warfare equal to the traditional domains, we—like those leaders—must vector it properly.

Toward that end, this article discusses airpower during the interwar period as well as key lessons learned that we can apply to the cyberspace domain. It then offers three suggestions that address the vectoring of the cyberspace domain: empowering commanders with actionable cyber intelligence, defending the nation with a combined civilian-military approach, and developing a long-term strategy for the domain by embracing the cyber culture and educating our young leaders in cyber. Understanding the past, applying lessons learned, and planning the way forward will allow us to secure true cyberspace dominance.

## The Interim Years of Airpower

Prior to World War I, the use of aircraft was extremely limited, and many people did not consider them a viable military option. For example, in *Aeronautics* (1908) William H. Pickering, a notable American astronomer, observed that "another popular fallacy is to suppose that flying machines could be used to drop dynamite on an enemy in a time of war."[1] Only six years later, on 14 August 1914, a French Voisin aircraft bombed German zeppelin hangars at Metz-Frascaty.[2] The idea of conducting aerial warfare quickly gained prominence. The next few

years saw the development of strategic-bombing aircraft and their use in air actions such as the raids by German Gothas on England.[3] However, the employment of aircraft and balloons in warfare was not new. In China during the third century, Gen Zhuge Liang signaled military forces and scared away enemies with balloons known as Kongming lanterns.[4] Yet, only advancements in technology and powerful demonstrations of force in World War I could expedite the domain's importance and use.

The success of airpower in that war, including Lt Frank Luke Jr.'s destruction of 14 heavily guarded German balloons, convinced several military leaders that aircraft could support the traditional domains of land and sea warfare.[5] The debate at the time did not concern whether or not to use airpower but the means of developing it and determining which branch of service would take the lead. In the years between the world wars, aviation concentrated on defending the nation from adversaries.[6] However, some of those defensive capabilities also offered offensive possibilities. The flexibility of airpower created intense debates between the Army and Navy because Army Air Corps aircraft could fill traditional Navy roles.

In 1921 General Mitchell used MB-2 bombers from Langley Field, Virginia, to sink three naval vessels, including the *Ostfriesland*, a modern battleship captured from the Germans.[7] This test demonstrated that aircraft could independently attack offshore targets. It also showed that if the Army continued to empower the Air Corps, the Navy might lose its primary mission of coastal defense.

Partially in rebuttal to General Mitchell's test, in 1925 the Navy revealed a plan to increase the number of its shore-based aircraft from 334 to 583.[8] Maj Gen Mason Patrick, chief of the Air Service, saw this as a move by the Navy Department to take control of the entire coastal defense mission.[9] This dispute between the Army and Navy continued to escalate, and leaders of both services worried that if they could not find a solution, Congress might create an independent air corps.[10] Attempts by the War Department and Congress to satisfy both services

proved fruitless.[11] Amidst the services' disagreement, General Mitchell strongly advocated the establishment of a separate branch of service and attempted to win the support of the public in an effort to pressure Congress to act.[12] After his court-martial, he resigned from the Army Air Service in 1926 but continued to campaign publicly for an independent Air Force.[13]

In 1934 Gen Henry "Hap" Arnold received a tasking to fly from Dayton, Ohio, to Alaska with 10 Martin B-10 bombers. On the return trip, he detoured from his route by flying over the ocean instead of across Canada, not only demonstrating the bombers' coastal range but also enraging Gen Douglas MacArthur, the Army chief of staff.[14] Nevertheless, members of Congress and the War Department ultimately embraced the claims of such individuals as Arnold and Mitchell that the nation needed an independent Air Force.

## Lessons Learned from Airpower

The cyberspace domain need not be a separate branch of service. However, the true potency of cyber power remains unrealized, as was the case with airpower in the early years of the aerial domain. If we understand this, we can extract key lessons learned from the nascent aerial domain and apply them to the development of the cyberspace domain.

### *Lesson One: A Unified Military Approach Is More Beneficial to Securing a Domain of Warfare*

One of the issues with realizing the potential of the aerial domain concerned early competition between the Army and Navy over its control—competition that led to creation of the Air Force. That service acted as a combined and vectored national approach to creating better aerial technologies and strategies. Had its establishment occurred sooner, the Air Force may have generated even more gains. In this way, cyber power has an advantage. The cyberspace domain does not encroach upon the traditional roles of the Army, Air Force, or Navy.

The cyber mission can work both independently from, and synergistically with, the traditional war-fighting domains across each branch. This combined approach from the services benefits the entire domain, and although we should encourage competition among the services, each one should play a significant role.

### *Lesson Two: Airpower Had the Ability to Make Influential Political Statements That Transcended Its Own Destructive Capability*

Cyber power, very much like airpower, can be a destructive force if wielded alone and to full measure. Early Airmen took pride in believing that aerial attacks by themselves could lead to victory; however, they understood neither its destructiveness if left unchecked nor the importance of limiting conflict.[15] During the Vietnam War, President Lyndon Johnson and Secretary of Defense Robert McNamara met weekly to discuss the targets that pilots would bomb. Once considered political micromanagement, this handpicking of targets controlled the political implications of aerial attacks.[16] The new—and in many cases frightening—power brought by bombing raids made a strong statement not only to North Vietnam but also to other nations watching closely. Similarly, cyber power can make influential statements, and we should not wield it indiscriminately. A cyber attack that collapses the global stock market, disables a fleet of naval warships, or crashes the latest development in aircraft will have enormous political consequences.

### *Lesson Three: Like Airpower, Cyber Power's Technologically Advanced Nature Allows It to Blur the Lines of War; Thus, We Must Wield It Responsibly*

Douhet believed that the range of aircraft would permit the targeting of civilians and combatants alike in future wars. Airpower, he reasoned, did not know the limits of traditional battlefields and could act without inhibition. Without boundaries on the battlefield, no areas would feel safe to civilians.[17] Cyber power, too, can quickly and specifi-

cally target networks and information systems throughout the world, blurring the lines of battlefields. This characteristic, in conjunction with its destructive force, generates fear of its capabilities among the population—one just as strong as that from terrorist attacks. Consequently, we cannot underestimate its power to influence popular opinion and politics or its ability to guide the development of cyber capability. When a nation uses cyber power, it must first carefully evaluate its own citizens' sense of security and the effects that cyber assets will have on that feeling after their employment.

### *Lesson Four: The Nature of War Is Not Limited by Technological Advancements*

Nevertheless, the idea that technology will eliminate the ugliness of war has influenced military planners throughout history.[18] Douhet believed that the inherently offensive nature of airpower, later famously reinforced by Sir Stanley Baldwin's statement that "the bomber will always get through," would curtail bloodshed during war.[19] To him, bombing cities and attacking civilians would result in fewer deaths than would the clash of armies.[20] The Italian general thought that strategic bombing would break the morale of civilians, prompting them to demand that their leaders end wars early. Instead, aerial bombing raids usually bolstered civilian morale against the known enemy.[21] Without proper attribution, though, in cyberspace the enemy may remain unknown, creating unspecified effects on the civilian population, perhaps including broken morale. Regardless of the effects of an unknown cyber attacker, technology cannot end bloodshed. Therefore, we must employ cyber's capabilities with the understanding that proper use can limit casualties but that overuse can equally encourage them. War will always be an ugly thing.[22]

### *Lesson Five: Airpower Used a Varied Approach to Secure the Domain, and So Must Cyber Power*

General Mitchell did not consider bombers the quintessential form of airpower, believing instead in the necessity of multiple types of aircraft, including those with offensive and reconnaissance missions.[23] His concept of airpower is more akin to the current diverse nature of cyber power and varied cyber assets, which can support national defense, intelligence gathering, and offensive actions—and do so just as well as or better than other military assets. Multiple types of aircraft enabled the development of persistent intelligence, surveillance, and reconnaissance (ISR) aerial platforms and offensive air capabilities, which help ensure air dominance and support to other war-fighting domains.[24] The addition of a variety of cyberspace capabilities directly enhances already-established ISR and offensive operations while enabling the development of new ones.

## Commanders and Actionable Cyber Intelligence

Vectoring the cyberspace domain should involve empowering commanders with more actionable intelligence through cyber capabilities. Cyber power offers critical advantages to campaign planning; consequently, intelligence-based cyber operations should become part of the preparation of the operational environment phase, which includes compromising enemy networks and readying cyber weapons for use in the event of conflict. During the posturing for offensive cyber operations, information exploited from compromised systems can aid in the joint intelligence preparation of the operational environment, improving commanders' situational awareness of the battlefield.[25]

Commanders use campaign planning to "synchronize efforts" and issue complementary guidance.[26] The two major phases of the planning process—contingency planning and crisis action planning—benefit from the timely information and attack options that cyber power pres-

ents, including an understanding of enemy capabilities and strategies. Having the assumptions and plans made in the contingency phase more closely match the crisis action phase expedites the joint operation planning process.[27] This quick-selection process empowers commanders with the ability to strike first, target precisely, and more readily defend counterattacks. Information gathered from the preparation of the operational environment phase also decreases the effectiveness of the enemy's attempts at deception.

With access to military doctrine, enemy forces may choose to avoid efficient courses of action or even fake them. The combination of cyber and ISR capabilities can detect these deceptions. Multiple ISR platforms such as manned aircraft, remotely piloted aircraft, and satellites, as well as human-gathered intelligence, contribute to creation of the intelligence preparation of the battlespace.[28] Individually, cyber and ISR severely weaken the enemy's ability to hide troops, sensitive information, operational plans, and centers of gravity. The combination of the two through imagery intelligence, signals intelligence, human intelligence, and computer network operations provides an unprecedented level of battlefield situational awareness to commanders. This awareness can also enable cyberspace operations, whose capabilities include weapon systems platforms that degrade, disrupt, and destroy an adversary's communication, control, and physical assets. The enhanced situational awareness that cyber and ISR give to commanders aids in creation of holistic and realistic statements of the commander's intent, as discussed in the joint operation planning process model. Better statements make the planning guidance more accurate and assist in the selection of effective courses of action.[29]

With adversaries relying heavily on cyberspace for communication, the number of capabilities offered to commanders to collect, exploit, and disrupt this information has never been greater. These options, which exist throughout all military operations, could help minimize what military theorist Carl von Clausewitz referred to as the fog of war.[30] However, many commanders cannot access them. If shared properly, cyber

operations would increase the chances for operational success in other domains and restrict the human and financial costs of war.

These cyber capabilities have not gone unnoticed, though, and the stand-up of US Cyber Command indicates that the cyberspace domain is moving in the right direction.[31] However, we need to do more to supply commanders with actionable intelligence and capabilities through cyber operations. Regarding the direction of cyberspace, Maj Gen Brett T. Williams, director of operations (J3) for US Cyber Command, called for empowering joint force commanders and combatant commands (COCOM) with cyber capabilities and command and control of cyber operations. A lack of visibility of cyber components critical to a mission's success puts commanders at a disadvantage. Major General Williams suggested creation of the Theater Cyber Operations Command, similar to a Theater Special Operations Command, to provide geographic combatant commanders with cyber capabilities under the control of COCOMs.[32] Establishing a method similar to this one would give commanders more actionable intelligence, and they could then request cyber capabilities relevant to their mission. Having the cyber situational awareness to accurately request capabilities is one of the most critical components of leveraging cyber power. This aspect has gained attention since Major General Williams made his observations. In the summer of 2011, Gen Keith Alexander, head of US Cyber Command, discussed progress in supporting operations in Iraq and Afghanistan through the deployment of expeditionary teams, especially in terms of combatant commanders' ability to request cyber support.[33]

Much work in the cyberspace domain remains with regard to delivering cyber intelligence and capabilities to commanders. After the establishment of more direct approaches for doing so, classification of the information becomes the limiting factor in making it actionable. To protect cyber capabilities, we must not reveal certain details and technologies that would allow adversaries to counter or safeguard against them. Currently, however, the intelligence and information gathered from cyber capabilities are overclassified. Commanders cannot request

capabilities they don't know about. Instead of providing processes to request cyber, we must make an effort to declassify cyber intelligence and information that does not weaken cyber capabilities. Doing so will not only support commanders but also enable tactical-level leaders to make reasonable requests to their leadership in support of daily operations. Moreover, the declassification of some cyber intelligence and information would allow more sharing among government agencies and civilian leaders who operate in law enforcement agencies. Perhaps even more important, the sharing of actionable cyber intelligence that could assist network defenses would enable civilian leadership to better protect sectors such as critical infrastructure. This sharing of information would directly correlate with improvements in national security.

## Cyber Weapons and the Home Front

During these interim years of cyberspace, increased civilian-military partnership for the defense of the nation would also prove advantageous. Recent cyber events have shown that the level of versatility and expertise in select cyber weapons can overpower even carefully crafted defenses. The combined experience and knowledge of military and civilian professionals can better protect against these advanced threats. No better example of advanced cyber threats currently exists than the dangers associated with Stuxnet.

In June 2010, the Stuxnet worm came to light and quickly gained notoriety as one of the most advanced pieces of malware ever discovered. The worm, which self-replicates and spreads among information systems, takes advantage of an unprecedented four unpatched vulnerabilities—known as zero-day vulnerabilities—while employing a root kit (a piece of code that enables persistent access), two command and control servers, and legitimate signed certificates.[34] The code consists of two sections: the weapon system and the payload, the former quite impressive and containing the aforementioned features but paling in comparison with the advanced nature of the payload.

Stuxnet was specifically designed to target supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS). More accurately, the payload specifically targeted programmable logic controllers (PLC) that governed the centrifuges at the Iranian nuclear facility in Natanz. The worm's payload physically damaged the centrifuges by spinning them up and slowing them down to precisely the appropriate speeds for maximum degradation.[35] Although the full outcomes of the worm remain unknown, satellite imagery indicates that over 1,000 of the centrifuges were destroyed.[36] This feat required not only some of the best programmers and ICS/PLC engineers in the world but also a better understanding of the secretive Natanz facility's layout than most of the engineers that worked there would have had.[37]

Largely seen as a cyber weapon created and employed by at least one nation-state, Stuxnet launched intense discussions and multiple academic papers on the use of cyberspace as a domain of warfare. The Russian ambassador to the North Atlantic Treaty Organization even went so far as to state that the Stuxnet worm could have caused "a new Chernobyl" if the program had released the uranium gas in the centrifuges instead of causing degradation.[38] Though operations had previously taken place in cyberspace, the media portrayal of the power of the Stuxnet cyber weapon made the discussion of cyber warfare a very public one. Stuxnet did for cyberspace what the early bombings in World War I did for airpower; that is, it brought the discussion to the public and undoubtedly forced many corporations and nation-states to research cyber capabilities more heavily. In a way, this event—coupled with past cyber operations over the last few decades, including the attacks against government and financial sectors in Estonia in 2007 and those that coincided with the Russian invasion of Georgia in 2008—represents the start of the interim years of cyberspace.[39]

Although Stuxnet infected and spread to thousands of computer systems, its only recognized targets were the centrifuges at Natanz. The event did not greatly affect systems in the United States or reach the level of a cyber attack that would push a nation into war. However, ac-

cording to Secretary of Defense Leon Panetta, "The potential for the next Pearl Harbor could very well be a cyber attack."[40] This observation, coupled with General Alexander's statements that segments of the nation's critical infrastructure are not prepared to handle cyber attacks and that this situation worries him the most, makes obvious the paramount importance of protecting these assets from cyber attacks.[41] Furthermore, Stuxnet has shown that these cyber capabilities exist and have been utilized by at least one nation-state.

The Stuxnet story is not over, though. The laboratory that discovered the piece of malware now known as Duqu on 14 October 2011 quickly recognized its relationship to the Stuxnet malware. Duqu differs from Stuxnet in that it is a targeted remote-access Trojan that steals information instead of a worm that damages centrifuges.[42] It infected a number of different sites, including universities, manufacturers, and certificate authorities in a style of attack that gathers data to use in making another Stuxnet-styled cyber weapon.[43] Although different in style and targets, Duqu uses much of Stuxnet's source code, and the same coding team, utilizing a common coding platform named Tilded, seems to have produced both pieces of malware.[44]

Similar to a "Lego set," the Tilded platform lends itself to putting together different pieces or modules of code to create entirely different malware.[45] This platform-based approach allows a team to create a quickly adaptable cyber weapon that can use different modules and payloads for employment against very different targets and produce different outcomes. Additionally, the malware created from the platform can be updated with different stealth measures, including the changing of encryption algorithms used to hide its code—as occurred with an updated version of Duqu found in February 2012.[46]

Aerial warfare has taken a platform-based approach to weaponry for years. Instead of creating aircraft with single functions, the Department of Defense (DOD) has purchased aircraft such as the F-16, F-22, and MQ-1, which can fulfill completely different mission sets based on their type of payload. Evidently this approach is now catching on in

the cyberspace domain, posing a number of risks to various aspects of national security. A single cyber weapon platform could steal information from universities and manufacturers to create multiple cyber weapons that would then attack aircraft, Internet nodes essential to command and control, air defense systems, and critical infrastructure.

Gen Norton Schwartz, former Air Force chief of staff, stated that the Air Force is pursuing "cyber methodologies to defeat airborne threats," but other sources have indicated that the technology is already available.[47] During testimony to the Senate Armed Services Committee, Lt Gen Herbert Carlisle stated that "the Russians and the Chinese have designed specific electronic warfare platforms to go after our high-value assets. Electronic attack can be the method of penetrating a system to implant viruses."[48] As traditional platform-based weapon systems become more diverse and utilize more capabilities, such as advanced radar systems, they become more vulnerable to cyber attacks. These cyber vulnerabilities make the benefits of cyber weapon platforms more alluring to adversaries. Such weaknesses, combined with the capabilities demonstrated by the Tilded platform, suggest that the threat of a future platform-based cyber weapon system attacking multiple DOD and civilian sectors is not merely possible but probable. We cannot defend against the power of such weapons without a combined military-civilian approach.

In these interim years of cyberspace, the government must ensure national security by encouraging cooperation with civilian leadership in sectors such as critical infrastructure. Operators, engineers, and developers of that infrastructure possess keen insight into the systems that demand active protection, yet they can supply full details about their systems and their understanding of them only when they receive actionable intelligence from the government. Armed with declassified intelligence, civilian counterparts can give better advice about defending systems they have operated for years. Just as it makes sense to classify some cyber offensive capabilities, so should we leave some cyber defense capabilities classified as well. Some cyber defenses,

though, should be largely transparent so that we can identify and remediate weaknesses.[49]

Even non-cyber-related ICS and SCADA system incidents can produce significant, drastic effects on civilian populations. On 17 August 2009, the 245-meter-high Shushenskaya dam—the largest in Russia—experienced an ICS failure that shook south central Siberia. A break in communications produced by a fire at a power station more than 500 miles away caused a sudden surge of water pressure that ripped apart a 940-ton turbine. The incident resulted in the death of 75 people and $1.3 billion in rebuilding costs.[50] Neither a cyber attack nor the action of any nation-state, the incident could have occurred as a result of a deliberate cyber strike and could have generated more civilian deaths and financial costs.

The Natanz nuclear enrichment facility and the Shushenskaya dam are only two examples of the uses of ICS and SCADA systems, which affect every aspect of daily life, including the stock market, oil industry, electrical power grid, water filtration, and Internet and satellite communication networks. Thus, these systems have become one of the most sought-after and viable targets of cyber weapons based in nation-states and must be treated accordingly. We can properly protect them only with a unified civilian-military approach.

## Winning the Next Generation

Lastly, embracing a long-term strategy for developing the cyber culture and educating the next generation of cyberspace operators, including the nation's youth, would help establish dominance in the cyberspace domain. Severe shortages exist in the availability of skilled cybersecurity professionals to fill such jobs as investigative forensics and programming at the FBI Cyber Division.[51] Further, the DOD finds itself in a difficult position in terms of educating the next generation. Dr. Michael Wertheimer, the National Security Agency's director of research and development, briefed members of the Senate Armed Ser-

vices Subcommittee on problems in recruiting and retaining professionals in computer science, pointing out that 77 percent of the agency's information technology staff resigns rather than retires.[52] We may need to address the issue of paying salaries competitive with those in private industry, but our long-term strategy must look to lessons learned from the aerial domain.

Excitement and a sense of magic surrounded airplanes and their pilots during the early days of airpower. Those flyers braved dangerous situations in an unchartered domain to break records and mesmerize crowds. France's Reims Air Meet of 22 August 1909, the world's first major air show, opened the door for many more around the globe.[53] Such shows and air races both inspired future pilots and educated the public on the capabilities of airpower.[54] The National Air Races, held in 1929 during the interwar years, attracted even more attention, drawing more than half a million people.[55]

The golden age of the 1920s embodied the allure of flying. Pilots wanted to fly higher, faster, and farther than anyone else. Three times between 1919 and 1921, Army pilots broke the world record for altitude.[56] Cyber operators, however, do not have to brave dangerous speeds and acrobatics, but cyber capabilities can certainly captivate audiences and inspire the next generation of cyber operators.

Hacking and security conferences demonstrate the latest in security advancements, vulnerabilities, and exploits. These conferences also offer a way for those in attendance to network with people from a variety of backgrounds who all have in common a certain passion for cyberspace. Unlike the early air shows, these conferences are neither inexpensive to attend nor embraced by the public. Although admission to some well-known conferences such as DEF CON is as little as $150, others require thousands of dollars, and optional training costs even more.[57] Granted, these prices reflect both the type of audience the event wishes to reach and operating costs, but persuading the mainstream public to attend cyberspace-related conferences presents a problem.

Other orchestrated conferences and advances in cyber-related education benefit the domain. The DOD's Cyber Crime Center hosts an annual cyber forensics challenge and convention that provide a wonderful opportunity to network, learn about the latest advances in technology, and sign up for training courses. The forensics challenge is free, but the well-intended and beneficial conference costs $500.[58] The government and DOD must host low-cost conferences akin to air shows where they can display capabilities and allow cyberspace to create its own sense of magic and allure.

With regard to making cyber deterrence more effective, Gen James Cartwright, USMC, retired, former vice-chairman of the Joint Chiefs of Staff, urged open discussion of and training in some cyber offensive capabilities.[59] Cyber conferences would be a perfect venue for members of the DOD to showcase some of the nation's cyber capabilities, attract audiences, and encourage the next generation while deterring adversaries. Moreover, cyber operators could offer these individuals low-cost or possibly free interactive, appealing classes on the fundamentals of cybersecurity and hacking, thus stimulating interest in the domain they will inherit.

Educating young people and stirring their interest in cyber are incredibly important. Although the DOD is deficient in this area, it is taking steps in the right direction in terms of educating and training young officers and enlisted members who have signed up to take part in the cyberspace domain. For example, the Air Force's Undergraduate Cyber Training technical school at Keesler AFB, Mississippi, which opened on 21 June 2010, offers cyber officers a six-month training course that concludes with students earning their cyberspace wings.[60] The schoolhouse fails students who do not pass the blocks of instruction, either retraining them into new Air Force specialty codes or separating them from the service.

The high-quality education offered at Undergraduate Cyber Training reflects the efforts of the faculty, made up of Air Force enlisted and officer personnel who have firsthand experience with and knowledge of

cyberspace operations. These instructors work to inspire and train the next generation of cyberspace officers as they put into practice General Schwartz's belief that a successful career should include a tour of duty as an instructor.[61] Doing so allows the faculty not only to sharpen their skills and academic pursuits but also to network and train with future squadron leaders. This networking creates buy-in from both the instructors and students, contributing to the overall cyber culture. The domain is infused with a sense of passion when instructors relate their experiences and students become excited about creating their own stories. Instructor pilots, war veterans, and participants in various cyber missions can inspire members of the next generation.

The early airpower culture even supported acts of defiance toward superiors and nonflyers to gain their peers' favor and reverence. Army Air Corps members would elevate their status by eliciting trouble and reprimand from Army leaders. They embraced the role of outcasts and found it empowering to create a diverse group and culture associated with flying.[62] Of course, military cyberspace professionals need not take such bold steps or challenge authority. The current military environment favors growth of the cyberspace domain, and, as mentioned previously, we do not need an independent cyber service. Nevertheless, members of the military cyberspace culture can feel very much like outcasts because of the domain's newness and its unexplored, misunderstood capabilities.

We must embrace, not shun, the infant cyber culture. Education and the fostering of a competitive, rewarding instructor-duty option for military members will permit the cyber culture to grow and develop. The best cyberspace operators should compete for duty as instructors and be rewarded with personal and career-enhancing opportunities. This will have the effect of continually updating the educational process and invigorating the cyberspace operators who participate. Consequently, a strong and unique cyber culture will develop, attracting and retaining passionate individuals dedicated to establishing cyber dominance.

## Conclusion

The cyberspace domain will forge its own place in history as a domain of warfare. However, similarities with the traditional war-fighting domains, especially the aerial domain, provide many lessons that leaders can use to guide the direction of cyberspace. By understanding these lessons and engaging in open dialogues about the direction of the domain from both a military and civilian perspective, we can apply the proper focus to cyberspace. Specifically, we must encourage actionable intelligence through cyber capabilities, the partnership of civilian and military professionals for national defense, and the cultivation of a cyber culture by means of educating the next generation.

Commanders must know what they can request in terms of support from cyber operators that will directly benefit their missions. Refraining from overclassifying information that pertains to cyber intelligence and cyber capabilities would empower leaders at the tactical, operational, and strategic levels and facilitate the sharing of information with civilian sectors to increase cyber awareness and create meaningful defense strategies. This would bolster national security by allowing civilian leaders to help defend their sectors instead of relying on the DOD and Department of Homeland Security. Lastly, by showcasing cyber capabilities and cyber intelligence at learning events and conferences, we could not only fortify cyber deterrence but inspire members of the next generation to take part in the cyberspace domain. Those individuals must remain the center of our long-term strategy for protecting the domain and establishing cyber dominance.

As General Alexander observed, "If people who seek to harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behavior change. The technology is ready."[63] Interested parties throughout the cyberspace domain, including the DOD, civilian sectors, and the next generation, are also ready for the challenges ahead. Cyber power is a powerful political and military tool that we must guide. We must also cement its place in history. The in-

terim years of cyberspace are taking place now, and leaders at all levels must act accordingly to ensure its future success. ✪

## Notes

1. William H. Pickering, "The Future of Artificial Flight," *Aeronautics* 6, no. 2 (1908): 17.
2. Alan Axelrod, *Little-Known Wars of Great and Lasting Impact: The Turning Points in Our History We Should Know More About* (Beverly, MA: Fair Winds Press, 2009), 222.
3. David Stevenson, *With Our Backs to the Wall: Victory and Defeat in 1918* (Cambridge, MA: Belknap Press of Harvard University Press, 2011), 186.
4. Andreas Wittmer, Thomas Bieger, and Roland Müller, eds. *Aviation Systems Elektronische Daten: Management of the Integrated Aviation Value Chain* (Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2011), 7.
5. "2nd Lt. Frank Luke Jr.," Official Web Site of the US Air Force, 2 November 2010, http://www.af.mil/news/story.asp?storyID=123006460.
6. Dr. James P. Tate, Lt Col, USAF, Retired, *The Army and Its Air Corps: Army Policy toward Aviation, 1919–1941* (Maxwell AFB, AL: Air University Press, 1998), 33, http://permanent.access.gpo.gov/websites/dodandmilitaryejournals/www.maxwell.af.mil/au/aul/aupress/books/tate/tate.pdf.
7. Capt B. Chance Saltzman and Thomas R. Searle, *Introduction to the United States Air Force* (Maxwell AFB, AL: Airpower Research Institute, College of Aerospace Doctrine, Research and Education, and Air University Press, 2001), 6, http://permanent.access.gpo.gov/websites/dodandmilitaryejournals/www.maxwell.af.mil/au/aul/aupress/books/searle/searle.pdf.
8. Tate, *Army and Its Air Corps*, 62.
9. Pamela Feltus, "Mason Patrick and the Creation of the U.S. Air Corps," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Air_Power/Patrick/AP15.htm.
10. Tate, *Army and Its Air Corps*, 67.
11. Ibid., 68.
12. Ibid., 190.
13. "Brig. Gen. William 'Billy' Mitchell," National Museum of the US Air Force, 11 February 2010, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=739.
14. Saltzman and Searle, *Introduction*, 12.
15. Col David A. Moore, USAF, *The Art of Aerial Warfare* (Maxwell AFB, AL: Air University Press, 2005), 17, http://dtlweb.au.af.mil///exlibris/dtl/d3_1/apache_media/L2V4bGlcmlzL2R0bC9kM18xL2FwYWNoZV9tZWRpYS81MDUxMg==.pdf.
16. Ibid., 19.
17. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC: Office of Air Force History, 1983), 9.
18. Moore, *Art of Aerial Warfare*, 68.
19. Sir Stanley Baldwin, "A Fear for the Future" (remarks to the House of Commons, London, 10 November 1932). See "The Bomber Will Always Get Through," *Air Force Magazine* 91, no. 7 (July 2008): 72, http://www.airforce-magazine.com/MagazineArchive/Documents/2008/July%202008/0708keeper.pdf.

20. Douhet, *Command of the Air*, 22–23.

21. Moore, *Art of Aerial Warfare*, 33.

22. John Stuart Mill, "The Contest in America," *Dissertations and Discussions*, vol. 1 (Boston: W. V. Spencer, 1868), 26.

23. David R. Mets, *The Air Campaign: John Warden and the Classical Airpower Theorists*, rev. ed. (Maxwell AFB, AL: Air University Press, 1999), 39, http://aupress.au.af.mil/digital/pdf/book/Mets_Air_Campaign.pdf.

24. Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower," *Joint Force Quarterly*, issue 60 (1st Quarter 2011): 47, http://www.ndu.edu/press/lib/images/jfq-60/JFQ60_46-53_Lambeth.pdf.

25. Joint Publication (JP) 5-0, *Joint Operation Planning*, 11 August 2011, III-9, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.

26. US Army War College, *Campaign Planning Handbook, AY 08 Final Working Draft* ([Carlisle Barracks, PA]: US Army War College, Department of Military Strategy, Planning, and Operations, 2008), vii, http://www.au.af.mil/au/awc/awcgate/army-usawc/campaign_planning_primer.pdf.

27. JP 5-0, *Joint Operation Planning*, IV-43.

28. Maj Eric D. Trias, PhD, USAF, and Capt Bryan M. Bell, USAF, "Cyber This, Cyber That . . . So What?," *Air and Space Power Journal* 24, no. 1 (Spring 2010): 95, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj10/spr10/aspj_en_2010_1.pdf.

29. JP 5-0, *Joint Operation Planning*, IV-41.

30. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 101.

31. "Cyber Command Achieves Full Operational Capability," news release no. 1012-10, US Department of Defense, 3 November 2010, http://www.defense.gov/releases/release.aspx?releaseid=14030.

32. Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Force Quarterly*, no. 61 (2nd Quarter 2011): 12, http://www.ndu.edu/press/lib/images/jfq-60/jfq-61/JFQ61.pdf.

33. GEN Keith B. Alexander, USA, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 4, http://www.au.af.mil/au/ssq/2011/summer/alexander.pdf.

34. Nicolas Falliere, Liam O Murchu, and Eric Chien, *W.32 Stuxnet Dossier*, Symantec Security Response, Version 1.4 (Cupertino, CA: Symantec Corporation, February 2011), 1–2, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

35. Ralph Langner, *Stuxnet Deep Dive*, video, 01:03:38, 31 January 2012, http://www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/.

36. Yaakov Katz, "Stuxnet May Have Destroyed 1,000 Centrifuges at Natanz," *Jerusalem Post*, 24 December 2010, http://www.jpost.com/Defense/Article.aspx?id=200843.

37. Langner, *Stuxnet Deep Dive*.

38. Ellen Messmer, "Stuxnet Could Have Caused 'New Chernobyl,' Russian Ambassador Says," *Network World*, 27 January 2011, http://www.networkworld.com/news/2011/012711-stuxnet-chernobyl.html.

39. Biony Kampmark, "Cyber Warfare between Estonia and Russia," *Contemporary Review* 289, no. 1686 (Autumn 2007): 288–93; and John Markoff, "Before the Gunfire, Cyberattacks,"

*New York Times*, 12 August 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1.

40. Jason Ryan, "CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor," *ABC News*, 11 February 2011, http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905#.T5M2ABHoK5I.

41. Charlie Rose, "Charlie Rose Talks to General Keith Alexander," *Bloomberg Businessweek*, 21 July 2011, http://www.businessweek.com/magazine/charlie-rose-talks-to-general-keith-alexander-07212011.html.

42. Boldizsár Bencsáth et al., *Duqu: A Stuxnet-Like Malware Found in the Wild*, Technical Report by Laboratory of Cryptography and System Security (Budapest: Budapest University of Technology and Economics, Department of Telecommunications, October 2011), 6–7, http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf.

43. "W32.Duqu: The Precursor to the Next Stuxnet," Symantec, 24 October 2011, http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet.

44. "Kaspersky Lab Experts: Duqu and Stuxnet Not the Only Malicious Programs Created by the Responsible Team," Kaspersky Lab, 29 December 2011, http://www.kaspersky.com/about/news/virus/2011/Kaspersky_Lab_Experts_Duqu_and_Stuxnet_Not_the_Only_Malicious_Programs_Created_by_the_Responsible_Team.

45. Rob Waugh, "Lethal Stuxnet Cyber Weapon Is 'Just One of Five' Engineered in Same Lab—and Three Have Not Been Released Yet," *Daily Mail*, 29 December 2011, http://www.dailymail.co.uk/sciencetech/article-2079725/Lethal-Stuxnet-cyber-weapon-just-engineered-lab.html.

46. Greg Masters, "Duqu Variant Uncovered," *SC Magazine*, 23 March 2012, http://www.scmagazine.com/duqu-variant-uncovered/article/233385/.

47. TSgt Richard A. Williams Jr., "CSAF Stresses Importance of Ready Future Force," Official Web Site of the US Air Force, 24 February 2012, http://www.af.mil/news/story.asp?id=123291264.

48. Eloise Lee, "Electronic Warfare Weapons," *Business Insider*, 15 March 2012, http://www.businessinsider.com/electronic-warfare-weapons-2012-3.

49. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 29.

50. Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no.1 (February 2012): 8, http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354.

51. Kevin Coleman, "Shortage of Adequately Trained Cyber Pros Puts US at Risk," *Defense Systems*, 22 June 2011, http://defensesystems.com/articles/2011/06/08/digital-conflict-cyber-worker-shortage.aspx.

52. Brian Donohue, "Experts Tell Senate: Government Networks Owned, Resistance Is Futile," *Threatpost*, 21 March 2012, http://threatpost.com/en_us/blogs/experts-tell-senate-government-networks-owned-resistance-futile-032112.

53. David H. Onkst, "Explorers, Daredevils, and Record Setters—an Overview," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/EX_OV.htm.

54. David H. Onkst, "The First U.S. Airshows—the Air Meets of 1910," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Explorers_Record_Setters_and_Daredevils/Early_US_shows/EX4.htm.

55. David H. Onkst, "Air Shows—an International Phenomenon," US Centennial of Flight Commission, accessed 20 September 2012, http://www.centennialofflight.gov/essay/Social/airshows/SH20.htm.

56. Tate, *Army and Its Air Corps*, 27.

57. "Official DEF CON FAQ," DEF CON, accessed 20 September 2012, https://www.defcon.org/html/links/dc-faq/dc-faq.html; and "Registration," Hacker Halted, accessed 20 September 2012, http://www.hackerhalted.com/2011/Registration.aspx.

58. "Registration," US Department of Defense, Cyber Crime Conference, 2013, http://www.dodcybercrime.com/12CC/registration.

59. Andrea Shalal-Esa, "Ex-U.S. General Urges Frank Talk on Cyber Weapons," Reuters, 6 November 2011, http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106?mid=520.

60. Bruce Rolfsen, "3,000 Officers Switch to Cyberspace Specialty," *Air Force Times*, 17 May 2010, http://www.airforcetimes.com/news/2010/05/airforce_cyber_careers_051710/.

61. Gen Norton A. Schwartz, chief of staff, to all Airmen, memorandum, 8 March 2012.

62. Tate, *Army and Its Air Corps*, 192.

63. Alexander, "Building a New Command," 9.

**1st Lt Robert M. Lee, USAF**

Lieutenant Lee (USAFA) is a flight commander at an intelligence squadron in Germany, working under the Air Force Intelligence, Surveillance, and Reconnaissance Agency. A graduate of the Air Force's Undergraduate Cyber Training technical school at Keesler AFB, Mississippi, he will receive an MS in cybersecurity / computer forensics from Utica College in the spring of 2013. Building on his passion for education, Lieutenant Lee founded a group that teaches free classes in cybersecurity, forensics, and hacking to on-base personnel in Germany. He has written articles on control-system cybersecurity, cyber warfare, nation-state cyber weapons of the future, and advanced cyber threats for publications such as *Control Global*, *SC Magazine*, *Australia Security Magazine*, and *Hong Kong Security Magazine*. He has also presented cyber-related topics at conferences in Miami, Florida; Seattle, Washington; Washington, DC; Prague, Czech Republic; Ramstein, Germany; Vienna, Austria; and London, England. Routinely consulted for his expertise on such subjects, Lieutenant Lee is an active cyber advocate.

**Let us know what you think! Leave a comment!**