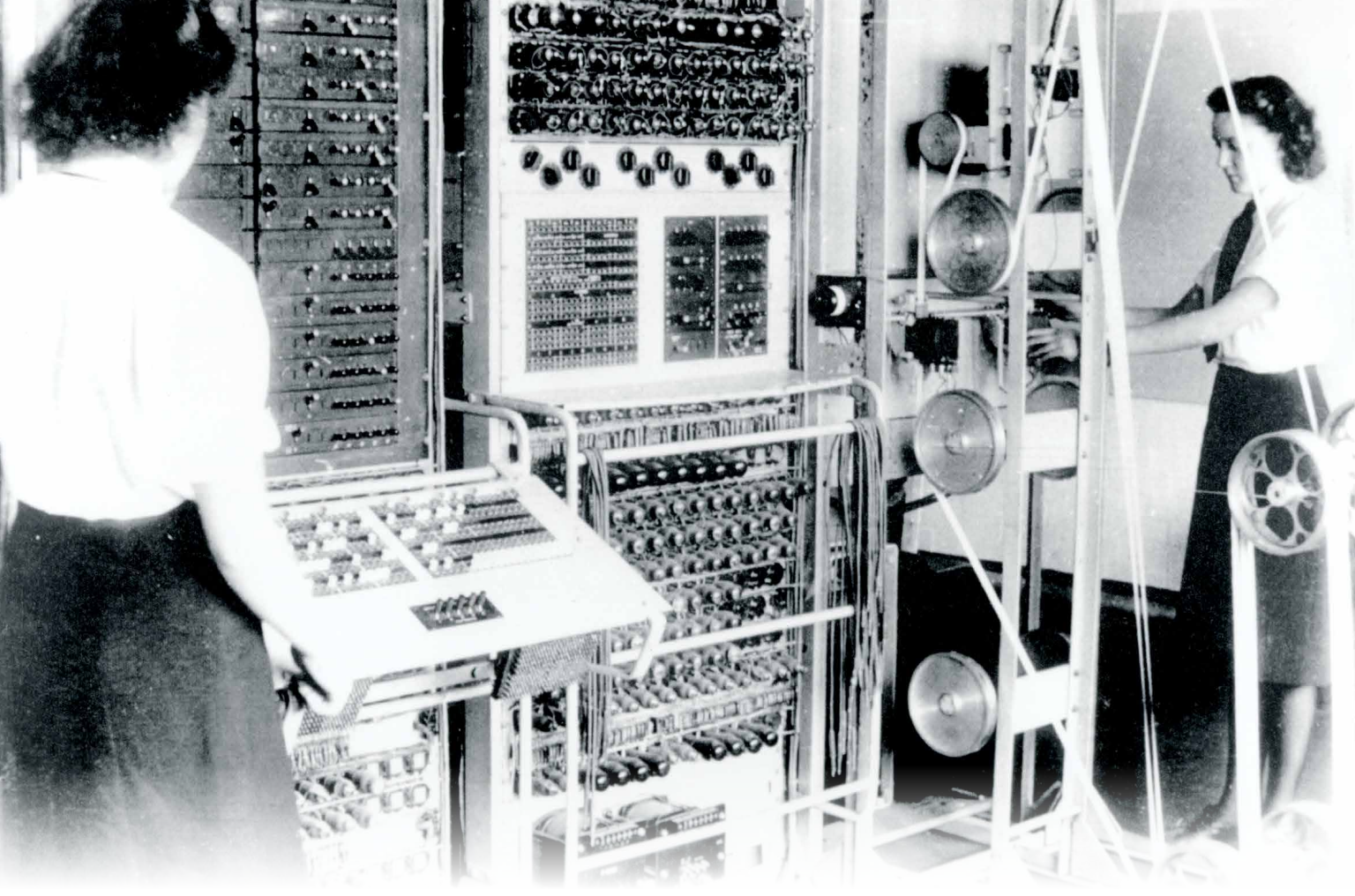


A Colossus Mark 2 codebreaking computer being operated by Dorothy Du Boisson (*left*) and Elsie Booker in 1943 at Bletchley Park, Buckinghamshire, England. (Photo courtesy of the United Kingdom National Archives) **Next page:** U.S. Cyber Corps insignia

Older Than You Realize

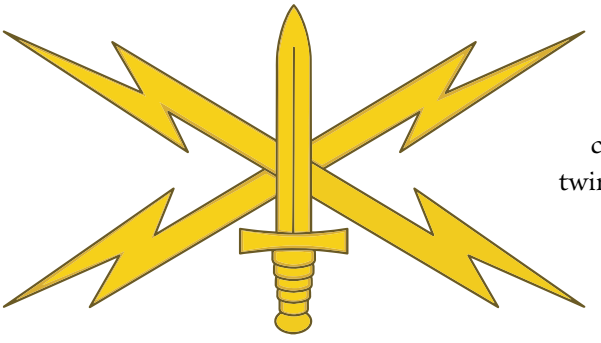
Teaching Branch History to Army Cyberwarriors

Scott Anderson

"So you are the Cyber Branch historian? That's cool, but I guess you don't have that much history to keep up with then."

I often hear similar comments when I explain my job title to people. To be fair, the U.S. Army Cyber School and Cyber Branch are just over six years old—mere embryos compared to the likes

of the infantry or cavalry. What bears explanation to skeptics is that while the Army's Cyber Branch is very young, the Department of Defense (DOD) effort to both protect networks and penetrate those of our adversaries goes back several decades. While the joint chiefs of staff may not have described cyberspace as a domain until 2004, the Soviets were paying hackers to steal U.S. military secrets as far back as 1986.[1] The birth of the Army's Cyber Branch in 2014 was merely a natural evolution in the need for the Army to codify the training standards and create a professional career path for its burgeoning corps of cyberwarriors who had until then been operating under the auspices of military intelligence (MI) units for some time.



The Cyber Branch Historian

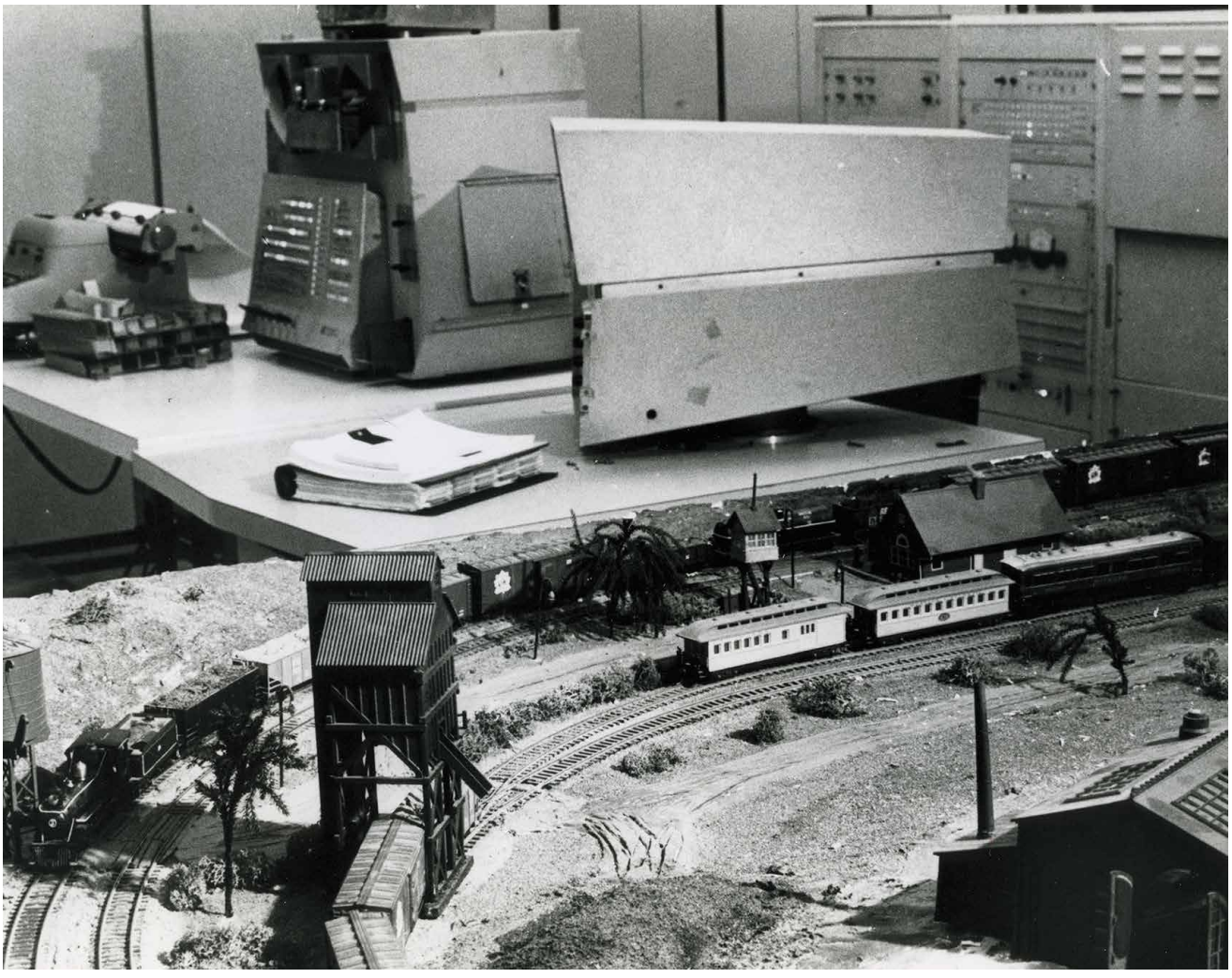
The U.S. Army Training and Doctrine Command's (TRADOC) Military History and Heritage Program oversees the requirements for Army branch historians. Every basic branch within the Army should have a historian working at its associated TRADOC school or center of excellence, and the young Cyber Branch is no exception. The Army Cyber School is located at Fort Gordon, Georgia, and nested within the Cyber Center of Excellence, which also operates the Army Signal School. The Cyber School, which officially opened in August 2014, had a historian on its staff by December 2015. Branch historians look to guidelines such as Army Regulation 870-5, *Military History: Responsibilities, Policies, and Procedures*; TRADOC Regulation 870-1, *United States Army Training and Doctrine Command Military History and Heritage Program*; and TRADOC Regulation 350-13, *Instruction in Military History*, for direction in their roles and responsibilities, with this latter regulation stipulating the categories of history instruction required for each type of professional military education class (e.g., Advanced Individual Training, Basic Officer Leaders Course, Warrant Officer Basic Course). Relevant branch history is among the required blocks for several of these classes, and it is here that I received my mandate to provide Cyber Branch history.

Creation of the Cyber Briefing

I developed a briefing for the officers, warrant officers, and enlisted soldiers at the U.S. Army Cyber School that would create an understanding of why their jobs exist and how many contemporary cyber events are not as new as they might think. This brief would be short if it only covered Army-related events, but as is the case with many aspects of the DOD's cyber mission, the milestones are of a joint nature. One of the unique things about cyber is that its history is intertwined with private-sector events and runs parallel in many instances with "hacking history." This hacking history, both in the military and the private sector, forms the basis for the briefing. What follows is a discourse on the content of the current cyber brief with an attempt to explain how past events in cyberspace (both military and private) have affected where we are today and why the U.S. Army has called cyberwarriors into service.

World War I

Cyber history begins here with World War I. The modern Cyber Branch of the U.S. Army originated from several of the duties and responsibilities formerly assigned to the Military Intelligence Corps and the Signal Corps. Gathering intelligence had always been a necessary component of warfare, but it was during World War I when the scale of information gathering reached unprecedented levels. From opening the citizenry's private mail to intercepting telegraph cables in order to gather secrets—or the inverse, cutting enemy cables to block communication—the origins of what we call "information warfare" were spawned during World War I. The predecessor of the National Security Agency (NSA), the ultrasecret Cipher Bureau headed by Herbert O. Yardley, came about in 1917. With the advent of radio and the ability to listen to an



A model railroad train set is in the foreground with a DEC PDP-1 console and monitor sitting on a table in the background in the Tech Model Railroad Club in 1961. (Photo courtesy of the Computer History Museum)

adversary's communications, the foundation of modern signals intelligence was also established.[2]

After the war, Yardley's Cipher Bureau, also known as "Black Chamber," set up a clandestine government cryptanalytic unit in a New York City building disguised as a commercial entity called the Code Compiling Company. Despite the chamber's success, the State Department shut it down in 1929 for several reasons, most famously after Secretary of State Henry L. Stimson stated, "Gentlemen do not read each other's mail." Disgruntled Yardley, out of a job, authored *The American Black Chamber* in 1931. The shocking exposé revealed the primary mission of the unit—the decryption of diplomatic communications of both friend and foe.[3]

World War II

Communications encryption became important in the early twentieth century, and with World War II came the advent of mechanized codebreaking. This codebreaking process was the focus at Bletchley Park, a nineteenth-century mansion and estate near London and the top secret headquarters of the British Government Code and Cypher School.[4] Among the scholars and academics turned codebreakers working in numbered huts at Bletchley, Alan Turing became the most known for his part in helping break the German Enigma code. Turing and his colleagues were depicted as breaking the Enigma by utilizing a "bombe" machine in the 2014 film *The Imitation Game*.[5]

The bombes were technically not computers but electromechanical devices that did not carry out calculations. However, another important machine developed at Bletchley Park is generally considered the first programmable electronic computer ever devised. With it, British cryptographer Tommy Flowers cracked an even more complex cipher machine known as the Lorenz, which carried communications of the German High Command—including Adolf Hitler. Flowers and his team dubbed their creation "Colossus," a project that remained a secret until the mid-1970s. Colossus was the first to utilize the modern binary system of ones and zeros that form the basis of modern computing.[6] Gen. Dwight Eisenhower reportedly gained confidence to launch the D-Day invasion on the Normandy beaches based on Colossus-intercepted messages confirming the Germans thought the invasion would be at Calais rather than Normandy.[7] William Friedman, perhaps America's most famous cryptologist and considered by many to be the father of modern cryptography, stated in 1942, "Actual physical warfare is intermittent, but mental, that is cryptanalytic warfare is continuous."[8]

> From opening the citizenry's private mail to intercepting telegraph cables in order to gather secrets—or the inverse, cutting enemy cables to block communication—the origins of what we call "information warfare" were spawned during World War I.

Postwar Developments

Early cryptography and mechanized codebreaking laid the foundation for the rapid postwar development of computers. The Army, in partnership with the University of Pennsylvania, built the first general purpose electronic computer. The previously mentioned Colossus had a specific task—codebreaking—while the new Electronic Numerical Integrator and Computer (ENIAC) handled a variety of tasks.[9] The ENIAC became operational in late 1945; its initial task was to calculate artillery firing tables for the U.S. Army's Ballistic Research Laboratory with a goal to both reduce calculation times and remove human error.[10]

"Cyber" entered the vernacular during the early postwar years via the concept of "cybernetics." This was the term coined by Massachusetts Institute of Technology (MIT) mathematician Norbert Weiner, whose interest in the new world of computing led to a new scientific discipline of sorts. Weiner took the Greek verb "kybernan," which means to steer, navigate, or govern, and attached his theory of cybernetics, promoting the idea that the most promising path for computer science was to devise machines that would work well with human minds rather than try to replace them.[11] While use of the word "cyber" as we use it today laid predominantly dormant until several decades later, Weiner's concepts serve as a conduit from the postwar rise of computers to modern day.

Turing theorized as far back as the 1930s about machine learning, but the 1950s are when artificial intelligence (AI) research began in earnest. During this decade, Turing developed his eponymously named "Turing Test," which evaluates a machine's ability to exhibit intelligent behavior equivalent to or indistinguishable from that of a human.[12] Dr. John McCarthy coined the term "artificial intelligence" in 1956, and along with Marvin Minsky, began the first coordinated AI research at MIT in 1959.[13]

Besides the aforementioned AI research program, MIT's Tech Model Railroad Club (TMRC) figures prominently in the early phase of cyber history. Founded in 1946, this club had two factions by the mid-1950s: those interested in the layout and painting of model trains and the "Signals and Power Subcommittee." The members of this latter group in many ways formed the nucleus of what became a recognized hacker culture within the United States. Members of the TMRC Signals and Power Subcommittee began applying the term "hacks" as early as 1955 to all manner of technology-based practical jokes and in the context of hacking the electrical system of their model railroads. In Steven Levy's thorough treatment of the TMRC in

Hackers: Heroes of the Computer Revolution, he explains that to qualify as a hack, the members felt that the feat must be innovative, stylish, and infused with technical virtuosity.[14] The members of the Signals and Power Subcommittee graduated in a sense from working on model train components to the early computers acquired by MIT. Their urge to learn coding and programming became so insatiable that they often forewent class attendance for precious time on the shared computer. One such member, Steve "Slug" Russell, even programmed the first computer video game in 1962 when he used MIT's PDP-1 computer to create *Spacewar!*[15] According to Levy, Russell and his fellow hackers also developed a silently agreed upon "hacker ethic."[16] These early computer enthusiasts called themselves hackers, but their "hacking" came mostly in the form of teaching themselves how to program these bulky computers to do things they were not intended to do, such as creating the aforementioned video game.

The first known public use of the term hacker in the modern vernacular came in the 20 November 1963 issue of MIT's newspaper, *The Tech*. The article described a criminal trespass, with hackers connecting the PDP-1 computer to the telephone system and launching a brute force attack, tying up all the phone lines between MIT and Harvard. In another act of ingenuity, the article explains that the hackers made long distance calls but charged them to a local radar installation.[17] This segues into an explanation of "phone phreaking" in the late 1960s and early 1970s, where crafty protohackers like John "Captain Crunch" Draper figured out how to replicate the precise 2,600 Hz tone needed to fool the Bell telephone system and make free calls around the world at a time when long-distance charges were at a premium and cell phones were nonexistent. In fact, whether using a computer, a "blue box," or even a toy whistle pulled from a Cap'n Crunch cereal box, making free long-distance phone calls became a rite of passage for many early hackers.[18]

Scott Anderson is the Army Cyber School and Cyber Branch historian at the Cyber Center of Excellence, Fort Gordon, Georgia. He holds an MA in public history from Middle Tennessee State University. His previous assignments include researching cases of World War II missing-in-action personnel for the U.S. military accounting mission and working for the U.S. Naval History and Heritage Command.

The Cold War

A concept now enters the discussion that really is at the heart of cyber—the development of networked computers. In many ways, the massive early warning radar system known as the Semi-Automatic Ground Environment, or SAGE, provided the foundation for linking many computer systems. Developed in the early years of the Cold War to warn of Soviet nuclear bombers entering North American airspace, SAGE consisted of hundreds of radar systems connected to large computer centers using an early modem capable of converting analog radar signals into digital code via telephone lines.[19] By the late 1960s, more and more organizations were linking their computer systems together via networks.

The DOD was no exception to this new practice that made for faster file sharing and collaboration within organizations. Willis Ware, an engineer for the RAND Corporation, could be considered the first computer security whistleblower. Ware delivered a paper at an academic conference in 1967 titled, "Security and Privacy in Computer Systems," which highlighted concerns with networked computers.[20] After Ware's warning, the DOD concerned itself with this new threat, even assembling a task force (with Ware as chairman) to recommend appropriate computer security safeguards. The task force report, published in February 1970, showed how corrupt insiders and spies could actively penetrate computers and steal or copy classified information.[21]

During the period that Ware and his team worked on their report, something truly monumental occurred that set the stage for practically everything that follows in the cyber chronology—the Advanced Research Projects Agency Network (ARPANET) established its first permanent link. The ARPANET, which was the precursor to our modern internet, was a computer network connecting American universities with defense research programs and the Pentagon. On 21 November 1969, this first permanent link was established between the University of California at Los Angeles (UCLA) and Stanford Research Institute (SRI) in Menlo Park, California, 367 miles apart. The network used packet switching, a new communications protocol that bundled a packet of data with its destination address. Every node on the network

An image of Cape Cod, Massachusetts, is displayed on screen in a Semi-Automatic Ground Environment (SAGE) control room during the Cold War. SAGE provided the foundation for linking many computer systems. (Photo courtesy of the U.S. Air Force)

passed on each packet until it reached its destination. This kept information flowing, with packets from one message filling in spaces between those of other messages so that each line could be used close to capacity. By 31 December 1969, ARPANET had expanded to four nodes: UCLA, SRI, the University of California at Santa Barbara, and the University of Utah.[22] By 1972, the "@" symbol was used to show that electronic messages were coming from a particular network, and by the following year, ARPANET users in the United States were corresponding with British researchers in real time over the Atlantic.[23]

Personal Computing

Since their development in the 1940s, computers steadily decreased in size from the mammoth ENIAC, which took up one thousand square feet of floor space, to the more compact but still refrigerator-size "minicomputers." The evolution from vacuum tubes to the transistor in 1948 and then to the microchip a decade later allowed the size of these machines to shrink while simultaneously increasing their speed and power. However, it was not until Intel's development of the microprocessor in 1971 that computers began transitioning to the compact sizes that we recognize as the personal computer.[24]

The cover story in the January 1975 issue of *Popular Electronics* magazine featured the "Altair 8800" and told how this simple looking small box with lights and switches rivaled the power of much larger commercial computers. Boyhood friends Bill Gates and Paul Allen later entered into a partnership with the Altair's makers to write the BASIC programming language, which in turn led to the formation of Microsoft.[25] Another famous duo in the development of personal computers, Steven Jobs and Stephen Wozniak, came out with the Apple I in 1976.[26] The 1970s witnessed several other firsts, including the first IRS computer embezzlement and the first hack into a government computer. And in 1979, a fifteen-year-old child became the first hacker to be arrested and charged with felony vandalism for disrupting a university's computer programs.

The 1980s

In 1983, the hit movie *WarGames* was released. If the previous decade had dabbled with the notion of teenagers getting smart on the new world of interconnected computer networks, this film amped up the theme to

the next level. *WarGames* stars Matthew Broderick as the typical hacker who nearly starts Armageddon from his bedroom when he begins playing what appears to be a new computer game called *Global Thermonuclear War*. However, he has unwittingly connected to an artificially intelligent computer with control over NORAD's nuclear arsenal. Interestingly, the film's writers consulted with the previously mentioned Willis Ware, who explained how the military's computers were at risk, giving them the confidence to move forward with their script.[27] While there are seemingly far-fetched aspects of this movie, it provides a case of pop culture influencing national policy. President Ronald Reagan watched *WarGames* shortly after its release and began asking whether something like what was depicted in the movie could really happen. Fifteen months later, his administration published National Security Decision Directive 145, *National Policy on Telecommunications and Automated Information Systems Security*.[28]

That same year, a group of real teenage hackers from Milwaukee calling themselves "The 414s" broke into several computer systems including the one in the Los Alamos National Laboratory. The FBI eventually caught up with them; foolishly, the group named themselves after their local area code.[29]

Solidifying 1983 as the year of the teenager hacker, CBS premiered *Whiz Kids* that fall, portraying a group of kids who routinely use hacking skills to assist the police in bringing criminals to justice.[30] Finally, to close out this monumental year, a graduate student named Fred Cohen created the first computer virus in November. Upon his proof-of-concept code taking over a mainframe within minutes at a computer security seminar, Cohen's academic advisor likened the self-replicating program to a "virus."[31]

The cyber milestones continued in the mid-1980s. The first large-scale data breach occurred in 1984 when hackers stole a file password from TRW, a large credit reporting agency that handled the confidential credit histories of over ninety million Sears customers on the West Coast. Utilizing a favorite communication medium of the early hacking age, the criminals posted the password on an electronic bulletin board providing like-minded individuals access to the exposed personal data.[32]

In 1986, the Soviets became involved in cyber espionage, but their participation was uncovered by American astronomer turned computer administrator Cliff Stoll. Well before our modern convenience of almost universal internet connection on a personal level, Stoll's employer, Lawrence Berkeley National Laboratory, received user fees from ARPANET patrons needing a network access point. Instead of ignoring a $0.75 billing discrepancy connected to one of these patrons, Stoll decided to dig. He connected the payment issue with a user moving through the network, suspiciously accessing several sites including the Army's unclassified portion of the ARPANET aptly named Military Network, or MILNET. Stoll employed many innovative tricks in an attempt to trace the hacker including setting up his pager to send alerts when the hacker logged in. Stoll eventually began sleeping at the lab for quicker response times, but his nemesis never stayed on the network long enough to get an accurate trace. Finally, Stoll concocted a plan that solidified his legacy. He planted juicy, albeit fake, documents in his network that the hacker could not resist, thus keeping him online long enough for an accurate trace. Known as a "honeypot," the technique is still part of the cyber toolkit today. In the end, Stoll's determination and innovation led to the capture of a West German hacker ring whose members sold stolen documents from U.S. military sites to the KGB. Stoll's 1989 book, *The Cuckoo's Egg*, chronicled these events, describing Russia's initial foray into cyber espionage. While the West Germans were caught and one member served prison time, the Russians were implicated in a type of spy craft they would eventually master.[33]

In the wake of Stoll's baptism by fire into this new world of cybersecurity, he became involved in helping solve other problems. He did not have to wait long for the next major incident: the "Morris Worm," which is considered the first large-scale malware attack in history.[34] On 2 November 1988, Robert T. Morris Jr., a Cornell University computer science graduate student, unleashed a self-replicating "worm" that did not destroy data but temporarily disabled about 10 percent of the internet, or about six thousand computers. One of the first people Stoll contacted upon learning of the problem was Robert H. Morris, who was not only the chief scientist at NSA's National Computer Security Center, but in an ironic twist, also happened to be the culprit's father! The younger Morris realized he was in trouble and confessed to his father, who could not help but feel a bit proud of his son's creation. Securing a lawyer, father and son went to the FBI. Morris's alleged goal was benign, to estimate the size of the internet, but a design error in his program

caused it to replicate out of control. Morris holds the distinction of being the first person found guilty by jury and convicted under the 1986 Computer Fraud and Abuse Act. He received three years' probation, four hundred hours of community service, and a $10,000 fine. A silver lining to this incident was the DOD's creation of the first computer emergency response team (CERT) at Carnegie Mellon University. Today, almost every country has a CERT, but in 1988, this important organization served as an around-the-clock cybersecurity response unit and raised public awareness about the vulnerabilities of connecting to the internet.[35]

It is safe to say that 2019 was the year of ransomware. That year saw an unprecedented number of attacks on state and municipal governments and agencies, healthcare providers, and educational establishments at a cost of over $7 billion.[36] However, the first case of ransomware occurred more than thirty years ago in a bizarre effort to boost AIDS research funding. During the second week in December 1989, Dr. Joseph Popp, a biologist working as a World Health Organization consultant in Africa, mailed over twenty thousand computer discs to business and government agencies in Europe, Africa, and Asia (none to the United States) under the guise of the "PC Cyborg Corporation." The recipients only saw a questionnaire about HIV when they popped in the discs, but after rebooting their computers ninety times, a hidden virus activated a file encryption program. Users then received a ransom note, promptly demanding a "licensing fee" of $189 for one year or $378 for lifetime access to their own files. Fortunately for the victims, most IT professionals easily bypassed the encryption, which meant Popp did not raise any research money. Popp was arrested and extradited to Great Britain but was deemed not mentally competent to stand trial.[37]

Impact of the World Wide Web

If 2019 marked the thirtieth anniversary of Popp's devious scheme, it also was the thirtieth anniversary of a more productive element within cyber history—the development of hypertext, the impetus for the creation of the World Wide Web. In March 1989, British computer scientist Timothy Berners-Lee submitted a proposal explaining his creation of hypertext to his bosses at the European

"President Ronald Reagan watched *WarGames* shortly after its release and began asking whether something like what was depicted in the movie could really happen. Fifteen months later, his administration published National Security Decision Directive 145, *National Policy on Telecommunications and Automated Information Systems Security*."

Cover art for *WarGames* courtesy of Metro-Goldwyn-Mayer

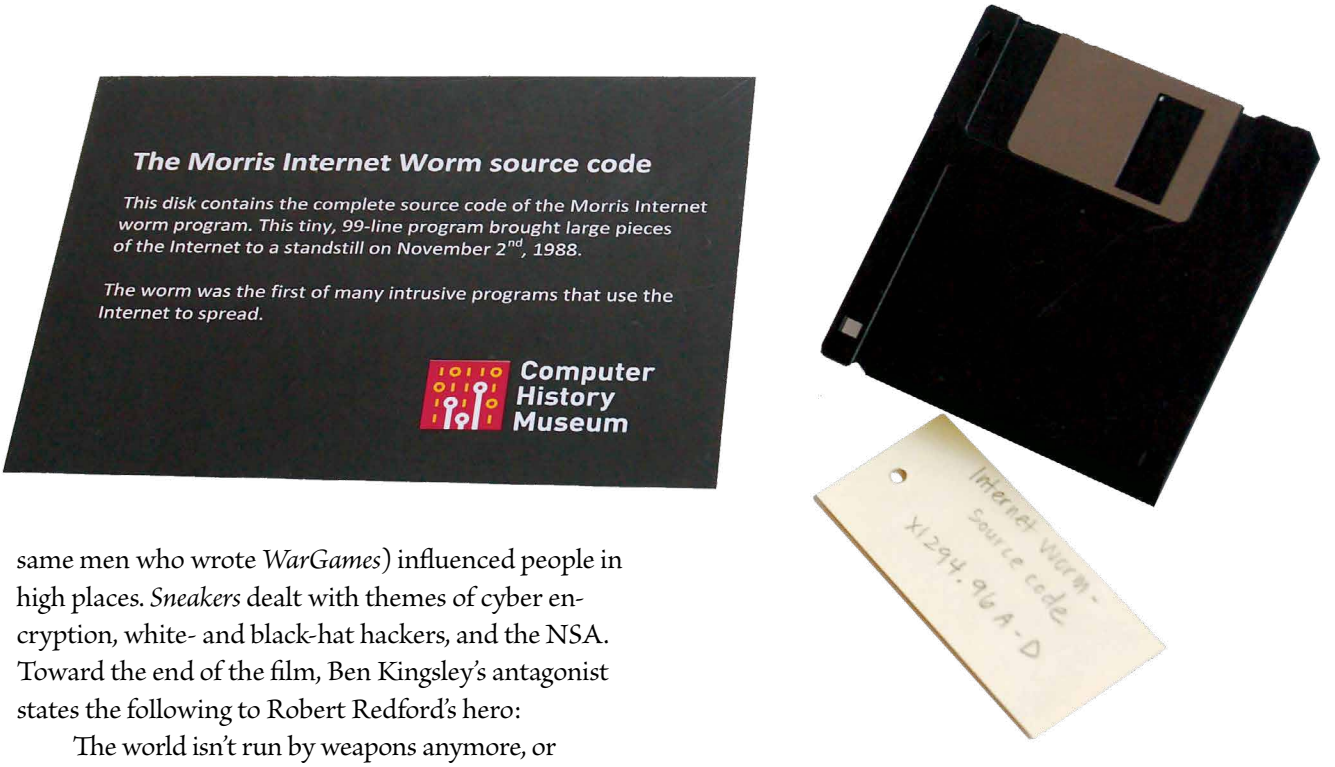
Council for Nuclear Research (CERN) in France. His idea for hypertext was to create words or phrases that were coded so that when clicked, the reader would be sent to another document or piece of content. When writing his initial proposal, the only name he had for it was "mesh," but soon after, he decided on "World Wide Web." He also created the term "uniform resource locator," more commonly known as URL, and a suite of tools that included "hypertext transfer protocol" (HTTP) and "hypertext markup language" (HTML), standard tools still in use today. The first website on the World Wide Web, a CERN page, went online two years later on 6 August 1991.[38]

With an increasing number of computer novices dialing into the World Wide Web in the early nineties, the average citizen became aware of issues related to privacy, identity theft, and hacking as they lived more of their lives "online." Hollywood followed suit with a slate of films such as *Hackers* and *The Net*, reflecting this new connected world. Reminiscent to the effect *WarGames* had on Reagan, the 1992 film *Sneakers* (cowritten by the same men who wrote *WarGames*) influenced people in high places. *Sneakers* dealt with themes of cyber encryption, white- and black-hat hackers, and the NSA. Toward the end of the film, Ben Kingsley's antagonist states the following to Robert Redford's hero:

> The world isn't run by weapons anymore, or energy, or money, it's run by little ones and zeroes, little bits of data. It's all just electrons … There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think … it's all about the information![39]

The NSA director at the time, Rear Adm. John Michael McConnell, saw the movie and was apparently convinced that the mission of the NSA needed to follow the key theme from the film, that "There's a war out there … It's all about who controls the information." Shortly thereafter, McConnell hired a director of information warfare within the NSA.[40]

The first large-scale DOD cyberattack exercise was orchestrated by the NSA—an event known as "Eligible Receiver." From 9 to 13 June 1997, NSA Red Team experts equipped with only off-the-shelf, publicly available computer equipment, began a systematic cyberattack against unsuspecting targets.[41] They targeted the electric grid first, and without flipping the switch, proved they could do so if they desired. Next came the Pentagon itself, which the testers thoroughly penetrated in four days. The Red Team compromised the U.S. military's command and control to the point that officials shut



A computer disk containing the Morris Internet Worm source code now found at the Computer History Museum in Mountain View, California. The worm was released 2 November 1988 and is considered the first large-scale malware attack in history. (Photo courtesy of the Intel Free Press via Flickr)

down Eligible Receiver early. The exercise proved there was much work to be done in cyberdefense.[42]

Government officials were still reviewing lessons learned from Eligible Receiver when the U.S. government faced major back-to-back cyberattacks in early 1998. In February, the Pentagon underwent the most organized and systematic attack on its unclassified computer systems to date. After the first week of attacks, DOD leaders took the unprecedented step to mobilize a special crisis cell on the joint staff under Operation Solar Sunrise to deal with the intrusions. In the end, the perpetrators were two California sixteen-year-old teenagers working with an eighteen-year-old Israeli.[43]

U.S. officials might have dodged a bullet with Solar Sunrise being the work of teenage pranksters, but no sooner had this event ended when administrators detected a more troubling intrusion that became known as Moonlight Maze. This new incursion was alarming enough that Deputy Secretary of Defense John Hamre briefed a congressional committee that "we're in the middle of a cyberwar."[44] Victims included the Pentagon, NASA, and the Department of Energy, just to name a few. The attacks persisted for several years, and most information is still classified, but in a somewhat odd metric provided, Moonlight Maze operators supposedly stole enough information that if printed on paper, the pile would stand three times higher than the Washington Monument.[45] Most evidence pointed to Russia; however, Moscow denied it, and the incident brought the problem of attribution to the forefront. The attack reinforced the reality that we were no longer just dealing with teenage hackers but state-sponsored attacks.[46]

In a signal that DOD officials had simply seen too much with the trifecta of cyber vulnerabilities revealed by Exercise Eligible Receiver, Solar Sunrise, and Moonlight Maze, they created Joint Task Force-Computer Network Defense (JTF-CND) in 1998, which reported to the secretary of defense and planted the seeds of an eventual national cyber command. This joint task force became the first organization with direct authority over operations on individual military service and DOD networks.[47] In June 1998, Company B, 742nd MI Battalion, 704th MI Brigade, was tasked to develop a computer network operations force.[48] This Fort Meade-based unit became the first Army unit dedicated to conducting cyber operations.

Twenty-First Century Cyber

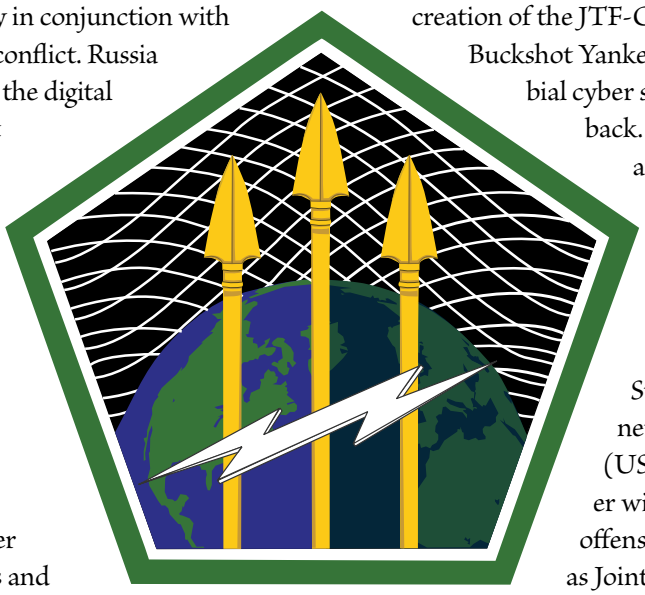
As the cyber chronology breached the twenty-first century, we saw the first real examination of hacking by the People's Liberation Army of China. Chinese patriotic hackers had struck U.S. websites, including the White House site, as early as 1999 in response to the accidental U.S. bombing of the Chinese embassy in Belgrade, Serbia, during the Kosovo conflict.[49] However, by 2003, the DOD was concerned with the first significant case of persistent Chinese cyberespionage. The U.S. codename for these intrusions was initially Titan Rain, with perhaps the most well-known target of these attacks being the Chinese theft of terabytes of data on the Joint Strike Fighter (F-35 Lightning II), which has suspiciously led to China's own development of similar stealthy fighters.[50] While Titan Rain was the first significant case of Chinese cyberespionage, it certainly was not the last.

The next major cyber milestone was triggered in 2007, oddly enough by a World War II-era statue located in the capital city of Tallinn, Estonia—a former Soviet republic. As Estonian leaders debated about the possible removal and relocation of the monument to the Liberators of Tallinn, which many viewed as a symbol of former Soviet repression, the Russian government warned that removing the statue would be "disastrous for Estonians."[51] Within hours after the statue's relocation from Tallinn's city square to a nearby military cemetery on 27 April, a widespread series of distributed denial of service attacks commenced against Estonia's computer networks. Lasting about three weeks, the attacks crippled much of Estonia's online infrastructure, including government services, online banking, and news media services. While the Russian government denied involvement, Vladimir Putin had fiercely criticized the statue decision. In the end, only one ethnic Russian Estonian was charged in relation to the attack. Before the incident, many considered Estonia the most "wired" country in Europe, but when the digital smoke cleared in the aftermath of what some nicknamed "Web War I," it was clear that this technologically progressive nation had not invested enough in cyberdefense.[52]

About fifteen months after the Estonia attacks, the world watched Russia become embroiled in another conflict with one of its former republics. The Russo-Georgian War lasted from 7 to 12 August 2008 over disputes in the Abkhazia and South Ossetia regions of Georgia. The

distributed denial of service attacks against Georgia had a whiff of familiarity to the Estonia attacks as Georgian online infrastructure such as government, news, and banking websites were hit. However, the incident quickly escalated to a shooting war as well, and it is considered by many to be the first time in history that cyber effects were used against an adversary in conjunction with conventional forces in armed conflict. Russia easily dominated both in both the digital and terrestrial battlespace, but another important aspect of the conflict is how Russia controlled the prevailing narrative available to the Georgians. The hacking became so pervasive that Russian propaganda allowed Moscow's version of events to dominate—a classic case of information warfare.[53]

Up to this point in the cyber narrative, the myriad breaches and hacks on U.S. government systems took place in the unclassified realm, never straying beyond (to our knowledge) the U.S. military's Nonclassified Internet Protocol Router Network, widely known as NIPRNet. However, in the fall of 2008, the DOD received a major wake-up call when a virus known as Agent.btz successfully penetrated not only NIPRNet but also the DOD's secret (SIPRNet) and top secret (Joint Worldwide Intelligence Communications System, or JWICS) systems. The standard unclassified version of the narrative involves curious DOD personnel stationed in the Middle East discovering an infected USB flash drive and inadvertently introducing the malware onto the network. While popping an unknown flash drive into a DOD computer was not acceptable in 2008, it is also likely that additional bad cyber hygiene promulgated the virus past the unclassified network. The virus was identified when the malware beaconed location information back to its creator, and the DOD responded with Operation Buckshot Yankee to fend off the attack. The United States never formally declared attribution to a specific nation, but there were several connections to Russia. As a result of this major incident, the DOD put new security procedures in place, including the banning of portable flash drives. Ultimately, Buckshot Yankee became the inspiration for centralizing the nation's cyber forces in a major new organization.[54]



U.S. Army Cyber Command Insignia

U.S. Cyber Command

As the milestone events Eligible Receiver, Solar Sunrise, and Moonlight Maze had prompted the creation of the JTF-CND a decade earlier, Buckshot Yankee seemed to be the proverbial cyber straw that broke the camel's back. Between November 2008 and June 2009, Secretary of Defense Robert Gates ordered directives connected to the creation of a new subunified command to operate under U.S. Strategic Command. The new U.S. Cyber Command (USCYBERCOM) came together with the merger of the existing offensive cyber organization known as Joint Functional Component Command–Network Warfare and the defensive Joint Task Force–Global Network Operations. On the day that Gen. Keith Alexander received his fourth star, the "dual-hat" arrangement between the NSA and USCYBERCOM was born, with Alexander leading both organizations at Fort Meade, Maryland. On 4 May 2018, USCYBERCOM became the Nation's tenth unified combatant command, no longer subordinate to U.S. Strategic Command.[55]

USCYBERCOM needed subordinate cyber units from all the service branches, and accordingly, the Army chief of staff approved the creation of a new separate command in early 2010. Headquartered at Fort Belvoir, Virginia, the new U.S. Army Cyber Command (ARCYBER) officially activated on 1 October 2010 with Lt. Gen. Rhett Hernandez as its first commanding general.[56] Two months later, the Army approved the establishment of its first dedicated cyber brigade, the 780th MI Brigade at Fort Meade.[57] The 780th falls administratively under the Intelligence and Security Command but operationally answers to ARCYBER.

ARCYBER announced in December 2013 that its base of operations would move to Fort Gordon, Georgia, and in September 2014, the Cyber Protection Brigade, which is ARCYBER's defensive cyberspace

operations unit, was activated at Fort Gordon.[58] Ground was eventually broken for the new ARCYBER headquarters in November 2016, and the official move took place in July 2020.[59]

One of the most analyzed cyber events in history is the Operation Olympic Games, better known as Stuxnet. While Pentagon officials have never officially taken credit or admitted any involvement in the creation of this virus that substantially set the Iranian nuclear program back, numerous articles and books contend that Stuxnet was an American/Israeli joint venture.[60] Regardless, the designers successfully infected Iran's Natanz uranium enrichment facility computer systems with a virus called the Stuxnet worm. During 2009 and 2010, the malware destroyed more than one thousand of the six-and-a-half-foot-tall aluminum centrifuges by causing them to spin out of control and be rendered useless. After Stuxnet accidentally spread beyond the Natanz facility due to a programming error, those studying the worm marveled at the sophistication of its design. Stuxnet is considered to be the first computer virus to go after industrial systems and cause actual damage to physical equipment. Stuxnet was a game changer, a point of no return that ushered in a new era in which warfare would never be the same.[61]

Chinese and Russian Attacks

Circling back to China and its hacking activities since the 2003 discovery of the aforementioned Titan Rain, that nation's hacking became synonymous with cyber espionage and the theft of both U.S. defense and private corporation secrets. Another cyber first occurred in May 2014 when the United States handed out the first-ever state-actor cyber espionage indictments against five Chinese People's Liberation Army officers for stealing data from six American commercial targets. U.S. authorities labeled the five officers as members of Unit 61398, also known as Advanced Persistent Threat 1, which is believed to be linked to the initial Titan Rain attacks.[62] Alexander believes China's estimated gains from economic espionage cost the U.S. hundreds of billions each year, calling it "the greatest transfer of wealth in history."[63]

In 2015, the U.S. Office of Personnel Management delivered the news that during the previous year, unknown but believed to be Chinese nationals hacked the Office of Personnel Management network, making off with the personal information of over twenty-one million Americans. The majority of victims were U.S. military and government employees who had applied for security clearances. Anyone who has ever filled out one of those forms knows the level of deeply personal background information required. Not only was China stealing defense and economic secrets, but now it also owned the most personally identifiable information of millions of Americans, which could be used for data mining or social engineering on a scale heretofore never seen.[64]

While the last five years have witnessed several major cyber events around the world, the last significant hacking event discussed in detail here is how Russia successfully flipped off the power switch in two areas of Ukraine during what some refer to as the Russo-Ukrainian War. After its annexation of Crimea in 2014, the Russian government launched a series of cyberattacks against the former Soviet republic including two significant wintertime power outages. On 23 December 2015, hackers shut down a significant part of Ukraine's electrical grid in the Ivano-Frankivsk region of western Ukraine, gaining access to thirty electricity substations. Over two hundred thousand people were left without electricity for a period of one to six hours during this first confirmed hack to take down a power grid.[65] Nearly a year later, just before midnight on 17 December 2016, another cyberattack shut down the power grid for part of the Ukrainian capital of Kyiv. Instead of gaining access to the Ukrainian utilities' networks and manually switching

off power to electrical substations, as hackers did in 2015, the 2016 attack was fully automated. It was programmed to include the ability to communicate directly to grid equipment, sending commands in the obscure protocols those controls use to switch the flow of power on and off. This power cut amounted to a loss of about one-fifth of Kyiv's power consumption at that time of night, and it lasted about an hour. As with the first attack, Russian hackers were suspected to be behind the attack, demonstrating their penchant for treating Ukraine as a cyber test lab.[66]

(Photo courtesy of the U.S. Army Cyber School)

Cyber School and Cyber Branch

On 20 February 2013, TRADOC commander Gen. Robert Cone gave an important briefing at the Association of the U.S. Army Symposium in Fort Lauderdale, Florida. In his briefing, he called for the formal creation of a cyber school and career field within the U.S. Army. He stated the Army needed to "start developing career paths for cyberwarriors as we move to the future."[67] On 25 June 2013, Army Chief of Staff Gen. Raymond Odierno approved the establishment of a consolidated Army Cyber School at Fort Gordon. The purpose of the Cyber School would be to unify and integrate training for the new cyber career field.[68]

The Army released executive order 057-14 on 24 January 2014, which officially changed the Signal Center of Excellence to the Cyber Center of Excellence and established the U.S. Army Cyber School at Fort Gordon. The Cyber Center of Excellence force modernization proponent included "cyberspace operations, offensive and defensive cyber operations, signal/communications networks and information services, and electronic warfare." The Cyber School mission was to "conduct analysis for the required training needed to develop a highly skilled cyber force, trained to joint standards and ready to meet combatant commanders' current and future force requirements."[69]

On 4 August 2014, Lt. Gen. Robert Brown, commanding general of the U.S. Army Combined Arms Center, which oversees the various Army centers of excellence, presided over a multifaceted transfer of

authority ceremony on Fort Gordon. During the ceremony, Col. Jennifer G. Buckner became the first chief of cyber and first permanent commandant for the new U.S. Army Cyber School. Later the same day, Buckner, a career MI officer, unveiled the Cyber School sign and cut the ribbon leading into the headquarters building.[70] However, the fanfare only lasted one day as the small staff immediately set to work planning the course maps for the school. Official branch creation came next, and when staff members handed Odierno the routing form with the draft orders on 31 August 2014, he initialed approval and added in bold letters: "Important and Historic!" The Army officially established the Cyber Branch as a basic branch of the Army the next day with the release of Department of Army General Orders 2014-63, signed by Secretary of the Army John McHugh.[71] Now branch officials could proceed with creating the 17-series career fields for officers (17A), warrant officers (170A), and enlisted soldiers (17C). In October 2014, the Army announced a Cyber Voluntary Transfer Incentive Program for active duty officers, second lieutenant through colonel, and by June 2015, the Army outlined guidance for warrant officers and enlisted soldiers desiring a transfer to the Cyber Branch.[72]

The Cyber Branch has a historical connection to the MI and Signal branches, and certain duties, functions, and positions associated with Army cyber operations were derived from career fields within the Signal and Military Intelligence Corps. A basic connection we can make when discussing these parent branches is that offensive cyberspace operations is a child of MI, and defensive cyberspace operations is the offspring of Signal.

On 26 May 2016, the lieutenants from the first Cyber Basic Officer Leadership Course class became the first to ever graduate a Cyber School course.[73] The first warrant officers graduated from Cyber Warrant Officer Advanced Course in August 2016, and October 2016 saw the activation of the Cyber Training Battalion, which manages the students while they are attached to the school.[74]

Army leadership then decided the electronic warfare functional area now belonged in the cyber realm as the Army resurrected it from the ashes of post-Cold War atrophy to what became a vital sphere in the era of remote-controlled improvised explosive devices during the Global War on Terrorism. All electronic warfare officers, warrant officers, and noncommissioned officers officially became members of the Cyber Branch on 1 October 2018.[75] In February 2017, top-secret-level course content became a reality with the opening of the Cyber Training Facility, and in early August 2017, the first 17C Advanced Individual Training class graduated.[76]

Another huge milestone occurred in October 2017 when the acting secretary of the Army approved a pilot program for direct commissioning of civilians with the right skills as officers in the Cyber Branch.[77] The first two direct commissioned officers were sworn in on 9 May 2018, breaking the centuries old Army tradition of only directly commissioning officers into the medical, legal, and religious fields during peacetime. Over two years into what was originally a pilot, the Army continues this program for cyber. While members of the Army Cyber Corps are in many ways still figuring out their identity and traditions, they can be proud of all that the branch has accomplished in such a brief period of time. ■

Notes

1. *The National Military Strategy of the United States of America: A Strategy for Today: A Vision for Tomorrow* (Washington, DC: Joint Chiefs of Staff, 2004), 1, accessed 25 August 2020, https://history.defense.gov/Historical-Sources/National-Military-Strategy/.

2. Gordon Corera, *Cyberspies: The Secret History of Surveillance, Hacking, and Digital Espionage* (New York: Pegasus Books, 2016), 10; John Finnegan, *Military Intelligence* (Washington, DC: U.S. Government Printing Office, 1997), 29.

3. Corera, *Cyberspies*, 40; Finnegan, *Military Intelligence*, 47–48; James Gilbert and John Finnegan, eds., *U.S. Army Signals Intelligence in World War II: A Documentary History* (Washington, DC: U.S. Government Printing Office, 1993), 26. In reality, the peacetime signals intelligence activities of the U.S. government did not stop. In 1929, the Signal Intelligence Service (SIS) was created to control all Army cryptology and absorbed the covert intelligence-gathering activities formerly conducted by the Black Chamber. The new unit, led by William Friedman, was set up within the Signal Corps rather than the Military Intelligence Division to reduce its visibility and better meet the technical requirements of signals intelligence. In Friedman's own words, the intercept activities of the SIS were technically illegal, so they stressed the idea that any intelligence was a byproduct of "training" in cryptanalysis.

4. "Cottage Industry," Bletchley Park, accessed 25 August 2020, https://bletchleypark.org.uk/our-story/why-it-matters/cottage-industry.

5. *The Imitation Game*, directed by Morten Tyldum, screenplay by Graham Moore (Santa Monica, CA: Black Bear Pictures, 2014).

6. Corera, *Cyberspies*, 26.

7. Ibid., 30–34.

8. Gilbert and Finnegan, *U.S. Army Signals Intelligence in World War II*, 26.

9. Walter Isaacson, *The Innovators: How a Group of Hackers, Geniuses, and Geeks, Created the Digital Revolution* (New York: Simon & Schuster, 2014), 79.

10. Ibid., 73.

11. Ibid., 222; Thomas Rid, *Rise of the Machines: A Cybernetic History* (New York: W. W. Norton, 2016), 3.

12. Isaacson, *The Innovators*, 124.

13. Ibid., 202; Martin Childs, "John McCarthy: Computer Scientist Known as the Father of AI," Independent, 1 November 2011, accessed 26 August 2020, https://www.independent.co.uk/news/obituaries/john-mccarthy-computer-scientist-known-as-the-father-of-ai-6255307.html.

14. Steven Levy, *Hackers: Heroes of the Computer Revolution*, 3rd ed. (Sebastopol, CA: O'Reilly Media, 2010), 10.

15. Ibid., 49–56.

16. Ibid., 27–31. Elements of this hacker ethic include (1) access to computers should be unlimited and total; (2) all information should be free; (3) mistrust authority; (4) hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position; (5) you can create art and beauty on a computer; and (6) computers can change your life for the better.

17. Henry Lichstein, "Telephone Hackers Active," *The Tech*, 20 November 1963, 1, accessed 26 August 2020, http://tech.mit.edu/V83/PDF/V83-N24.pdf.

18. For an exhaustive study on phone phreaking, see Phil Lapsley, *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell* (New York: Grove Press, 2013).

19. "SAGE: Semi-Automatic Ground Environment Air Defense System," Lincoln Laboratory, Massachusetts Institute of Technology, accessed 27 August 2020, https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system; Isaacson, *The Innovators*, 225–26.

20. Willis H. Ware, "Security and Privacy in Computer Systems" (lecture, Spring Joint Computer Conference, Atlantic City, NJ, 17–19 April 1967), accessed 27 August 2020, https://www.rand.org/pubs/papers/P3544.html.

21. *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security* (Washington, DC: RAND Corporation, 11 February 1970), accessed 27 August 2020, https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ware70.pdf.

22. Carl Stieren, "ARPANET, Forerunner of the Internet, Becomes Permanent," It Happened in the 60s, 20 November 2012, accessed 27 August 2020, http://www.ithappenedinthe60s.com/posts/november-21-1969/#:~:text=By%20Dec.,and%20the%20University%20of%20Utah.

23. Corera, *Cyberspies*, 81.

24. Isaacson, *The Innovators*, 197–99.

25. H. Edward Roberts and William Yates, "ALTAIR 8800: The Most Powerful Minicomputer Project Ever Presented-Can Be Built for Under $400," *Popular Electronics* 7, no. 1 (January 1975): 33–38, accessed 27 August 2020, http://www.computermuseum.20m.com/popelectronics.htm; Isaacson, *The Innovators*, 337.

26. Levy, "Woz," chap. 12.

27. Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 1, 9–10.

28. Ibid., 1–2.

29. Timothy Winslow, "I Hacked into a Nuclear Facility in the '80s. You're Welcome," CNN, 3 May 2016, accessed 27 August 2020, https://www.cnn.com/2015/03/11/tech/computer-hacker-essay-414s/index.html.

30. Sally Bedell Smith, "CBS is Revising Show on Computer Tampering," *New York Times* (website), 1 September 1983, accessed 27 August 2020, https://www.nytimes.com/1983/09/01/arts/cbs-is-revising-show-on-computer-tampering.html.

31. Kim Zetter, "Nov. 10, 1983: Computer 'Virus' is Born," *Wired* (website), 10 November 2009, accessed 27 August 2020, https://www.wired.com/2009/11/1110fred-cohen-first-computer-virus/.

32. Stuart Diamond, "Credit File Password is Stolen," *New York Times* (website), 22 June 1984, accessed 27 August 2020, https://www.nytimes.com/1984/06/22/business/credit-file-password-is-stolen.html.

33. For more details on Stoll's persistent investigation into the hacker, see Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Doubleday, 1989); or the shorter article, Clifford Stoll, "Cuckoo's Egg: Stalking the Wily Hacker," in *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, ed. Jason Healey (Vienna, VA: Cyber Conflict Studies Association, 2013), 89–106.

34. Stoll described his investigation into the "Morris Worm" incident in the epilogue of Stoll, *The Cuckoo's Egg*, 308–23.

35. Robert T. Morris eventually became a tenured professor in the Electrical Engineering and Computer Science Department at the Massachusetts Institute of Technology. For more details on the "Morris Worm" incident, see Corera, *Cyberspies*, 131–45.

36. "The State of Ransomware in the US: Report and Statistics 2019," EMISOFT Blog, 12 December 2019, accessed 27 August 2020, https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/.

37. Kaveh Waddell, "The Computer Virus that Haunted Early AIDS Researchers: The First-Ever Ransomware Attack was Delivered on a Floppy Disk," *The Atlantic* (website), 10 May 2016, accessed 27 August 2020, https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/.

38. Isaacson, *The Innovators*, 410–14.

39. *Sneakers*, directed by Phil Alden Robinson (Los Angeles: Universal Studios, 1992).

40. Kaplan, *Dark Territory*, 31–32.

41. Joint Publication 2-0, *Joint Intelligence* (Washington, DC: U.S. Government Printing Office, 22 October 2013), GL-11. Red teaming is defined as "an organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others."

42. Kaplan, *Dark Territory*, 68–70; Corera, *Cyberspies*, 171–72.

43. Tim Maurer, "SOLAR SUNRISE: Cyber Attack from Iraq?," in Healey, *A Fierce Domain*, 121–35.

44. Newsweek Staff, "We're in the Middle of a Cyberwar," *Newsweek* (website), 19 September 1999, accessed 28 August 2020, https://www.newsweek.com/were-middle-cyerwar-166196.

45. "Moonlight Maze Lives On? Researchers Find 20-Year-Old Link to Current APT," Secure World, 3 April 2017, accessed 28 August 2020, https://www.secureworldexpo.com/industry-news/moonlight-maze-lives-on-researchers-find-link-to-current-apt.

46. Adam Elkus, "Moonlight Maze," in Healey, *A Fierce Domain*, 152–63.

47. Healey, *A Fierce Domain*, 44–47; "U.S. Cyber Command History," U.S. Cyber Command (USCYBERCOM), accessed 28 August 2020, https://www.cybercom.mil/About/History/.

48. "History," 780th Military Intelligence (MI) Brigade, accessed 28 August 2020, https://www.inscom.army.mil/msc/780mib/history.html.

49. Healey, *A Fierce Domain*, 51.

50. Corera, *Cyberspies*, 189; "After Copying F-35's Stealth, China's J-20 Duplicating its Non-Stealth Features," DefenseWorld.net, 4 June 2020, accessed 28 August 2020, https://www.defenseworld.net/news/27131/After_Copying_F_35_s_Stealth__China_s_J_20_Duplicating_its_Non_Stealth_Features.

51. Joshua Davis, "Hackers Take down the Most Wired Country in Europe," *Wired* (website), 21 August 2007, accessed 28 August 2020, https://www.wired.com/2007/08/ff-estonia/.

52. Andreas Schmidt, "The Estonian Cyberattacks," in Healey, *A Fierce Domain*, 174–77.

53. Kaplan, *Dark Territory*, 164–65.

54. Karl Grindal, "Operation BUCKSHOT YANKEE," in Healey, *A Fierce Domain*, 205–11.

55. USCYBERCOM, "U.S. Cyber Command History."

56. "History," U.S. Army Cyber Command, accessed 28 August 2020, https://www.arcyber.army.mil/Organization/History/.

57. 780th MI Brigade, "History."

58. Subordinate units of the 780th MI Brigade are the 781st MI Battalion at Fort Meade and the 782nd MI Battalion at Fort Gordon; Neil Guillebeau, "Army Cyber Brigade Activates at Fort Gordon," Army.mil, 12 September 2014, accessed 28 August 2020, https://www.army.mil/article/133614/army_cyber_protection_brigade_activates_at_fort_gordon.

59. Wesley Brown, "Army Cyber Command Announces Fort Gordon as New Headquarters," *Augusta Chronicle* (website), 19 December 2013, accessed 31 August 2020, https://www.augustachronicle.com/article/20131219/NEWS/312199907; "Groundbreaking Marks 'Leap Forward' for Army Cyberspace Operations," Army.mil, 1 December 2016, accessed 28 August 2020, https://www.army.mil/article/178917/groundbreaking_marks_leap_forward_for_army_cyberspace_operations; "Army Cyber Command Ceremony Heralds Its Arrival at New Headquarters at Fort Gordon," Army.mil, 24 July 2020, accessed 28 August 2020, https://www.army.mil/article/237570/army_cyber_command_ceremony.

60. One example is David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), 9.

61. For more reading on Stuxnet, see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Crown, 2014); Kim Zetter and Huib Modderkolk, "Revealed: How a Secret Dutch Mole Aided the U.S.-Israeli Stuxnet Cyberattack on Iran," Yahoo! News, 2 September 2019, accessed 28 August 2020, https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html.

62. Sanger, *The Perfect Weapon*, 119–20; "What Is an Advanced Persistent Threat (APT)?," Kaspersky, accessed 3 September 2020, https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats. According to Kaspersky, an APT is an "advanced persistent attack using clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences."

63. Adam Segal, "From TITAN RAIN to BYZANTINE HADES: Chinese Cyber Espionage," in Healey, *A Fierce Domain*, 173.

64. Sanger, *The Perfect Weapon*, 111–17.

65. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* (website), 3 March 2016, accessed 28 August 2020, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

66. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired* (website), 20 June 2017, accessed 28 August 2020, https://www.wired.com/story/russian-hackers-attack-ukraine/.

67. "Army Leaders See Much Cyber Work to Do," Taktik(z), 24 February 2013, accessed 16 February 2017, http://taktikz.com/2013/02/24/army-leaders-see-much-cyber-work-to-do/.

68. "New Center, School to Bring Signals, Cyber, EW Together," *Military Times* (website), 25 June 2013, accessed 28 August 2020, https://www.militarytimes.com/2013/06/25/new-center-school-to-bring-signals-cyber-ew-together/.

69. Headquarters Department of the Army Executive Order 057-14, "Cyber Center of Excellence (COE) Establishment," 24 January 2014.

70. Meg Mirshak, "Fort Gordon Unveils U.S. Army Cyber School Headquarters," *Augusta Chronicle* (website), 4 August 2014, accessed 8 January 2016, https://www.augustachronicle.com/article/20140804/NEWS/308049896.

71. John M. McHugh, Department of the Army General Orders (DAGO) 2014-63, "Establishment of the United States Army Cyber Branch," 21 August 2014.

72. Officer - Military Personnel (MILPER) Message 14-298, 8 October 2014; Enlisted - MILPER Message 15-164, 2 June 2014; Warrant Officer - MILPER Message 15-166, 4 June 2015.

73. Laura Levering, "Army Cyber School Marks Major Milestone," Army.mil, 17 August 2015, accessed 28 August 2020, https://www.army.mil/article/154001/Army_Cyber_School_marks_major_milestone/.

74. Danielle S. Covington, "Cyber Training Battalion Activates," *Fort Gordon Globe* (website), 14 October 2016, accessed 31 August 2020, https://www.fortgordonnews.com/articles/cyber-growth-2/.

75. Nick Spinelli, "Cyber Celebrates 4 Years, Welcomes New Branch," *Fort Gordon Globe* (website), 5 October 2018, accessed 31 August 2020, https://www.fortgordonnews.com/articles/cyber-celebrates-4-years-welcomes-new-branch/.

76. Nefeteria Brewster, "Fort Gordon Graduates First Class for Cyber School," *Augusta Chronicle* (website), 8 August 2017, accessed 9 September 2020, https://www.augustachronicle.com/news/2017-08-08/fort-gordon-graduates-first-class-cyber-school.

77. Ryan D. McCarthy, Memorandum for Principal Officials of Headquarters, Department of the Army, "Army Directive 2017-26 (Pilot Program for Direct Commission to Cyber Positions)," 27 October 2017 (superseded).