



VICTORY IN CYBERSPACE



OCTOBER 2007

AN AIR FORCE ASSOCIATION SPECIAL REPORT



The Air Force Association

The Air Force Association (AFA) and its affiliate Aerospace Education Foundation (AEF) consolidated in 2006 to blend the two organizations into one with a great amount of value added to our programs and for members and prospective members.

The mission of AFA has always been to **EDUCATE** the public about the critical role of aerospace power in the defense of our nation, to **ADVOCATE** aerospace power and a strong national defense, and to **SUPPORT** the United States Air Force and the Air Force family. The new AFA will still maintain this mission but will include a much stronger focus on education, specifically the importance of science and math for the future of our country's national defense, and providing scholarship support for the Air Force family. Through this, we will support our airmen and their families as well as the many who are touched by our education outreach programs.

The consolidation of our two organizations allows AFA to become a 501(c)(3) charitable educational organization, in which all donations are tax deductible. With your help we will be able to expand our programs and their impact on those who participate in them. We need your support and ongoing financial commitment to realize our potential.

AFA disseminates information through *Air Force Magazine*, *Air Force Magazine Online*, the Eaker Institute, public outreach, and national conferences and symposia. Learn more about AFA by visiting us on the Web at www.AFA.org.

About the Author: DR. REBECCA GRANT is president of IRIS Independent Research, Inc., in Washington, D.C., and a fellow of the Eaker Institute, the public policy and research arm of the Air Force Association. She is also contributing editor to *Air Force Magazine*, the journal of the Air Force Association, and has worked for RAND, the Secretary of the Air Force, and the Chief of Staff of the Air Force. Her professional research interests center on joint doctrine and airpower employment in joint campaigns.

© 2007 Air Force Association

Published by the Air Force Association
1501 Lee Highway
Arlington VA 22209-1198
Tel: (703) 247-5839
Fax: (703) 247-5853

Produced by the staff of *Air Force Magazine*
Design by Darcy Harris
Cover composite by Darcy Harris; F-22A USAF photo/
TSgt. Ben Bloker

VICTORY IN CYBERSPACE

BY REBECCA GRANT

OCTOBER 2007

AN AIR FORCE ASSOCIATION SPECIAL REPORT

For 53 years, not one American soldier has died as a result of enemy aircraft fire. I aim to extend this hard-earned dominance for another 53 years and more, and use cyber and space power to do it.—Secretary of the Air Force Michael W. Wynne, West Point, N.Y., Sept. 11, 2006.

“America is under widespread attack in cyberspace.” That warning came from then commander of US Strategic Command, Marine Corps Gen. James E. Cartwright, in a March 2007 statement. Cartwright warned, “Unlike in the air, land, and sea domains, we lack dominance in cyberspace and could grow increasingly vulnerable if we do not fundamentally change how we view this battlespace.”¹

The world of cyberspace is no longer an untarnished, virtual place where common interests and collaborative protocols prevail. Five or 10 years from now, senior defense officials believe, an adversary may not need soldiers, ships, or aircraft to strike hard at the United States. The preferred tool may be information-based attacks carried out in cyberspace—a domain of information storage and relay that exists in wide area networks such as the Internet and restricted military and government systems. Targets of these enemies may be military forces, critical infrastructure, or commercial entities. The attacks may come in relentless waves or be over in seconds. Perhaps there will be no explosions and no shedding of blood, but attackers will still “close with and destroy” the enemy by having an incapacitating impact on the flow of information.

Two years ago, the US Air Force staked its claim to the cyberspace mission. The idea of fighting in cyberspace as well as in air and space was central to a new mission statement released in December 2005 by Air Force Secretary Michael W. Wynne and Air Force Chief of Staff Gen. T. Michael Moseley. Shortly thereafter, the Air Force also decided to reorganize its cyber capabilities and prepare to stand up a major command dedicated to arming, training, and equipping forces for operations in cyberspace. According to an Air Force estimate, as many as 40,000 airmen already have a role in cyberspace operations.

“The mission statement came from a recognition that everything we do requires integrated cyber capabilities,” says Air Force Lt. Gen. Robert J. Elder, who, as commander of the 8th Air Force, was handed the reins to the Air Force’s cyber capabilities.² He had earlier said that the point of the new venture is “about really ensuring that we can continue to function as a superpower.”³

A DOMAIN OF ITS OWN

Just how did the domain of cyberspace come to be on a par with the traditional domains of air and space? Equally important, how does that development affect the airman’s profession?

The official Department of Defense dictionary defines cyberspace as “a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.” Of course, the Air Force (and other services) has been exploiting parts of the electromagnetic spectrum for decades. What has lately turned cyberspace into a domain is the transfer of critical functions—military and commercial—into this collection of networks. Cyberspace functions are now tightly integrated with those carried out in air and space. In fact, the Air Force’s formation, over the past decade, of secure networks for expeditionary operations has become central to the way it fights. This fact was only too obvious in the way the Air Force fought at the start of Operation Iraqi Freedom in 2003.

Cyberspace may be a single medium, but it has multiple theaters of operation. The Internet is not the full story of the cyberspace domain. The Internet and military cyberspace can and should be thought of as two distinct areas of responsibility (AORs). At the same time, cyberspace has become an arena

1. Gen. James E. Cartwright, commander, US Strategic Command, testimony, House Armed Services Committee, March 8, 2007.

2. Author interview, Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, July 25, 2007.

3. Lt. Gen. Robert J. Elder Jr., Defense Writers Group roundtable, June 13, 2007.

where various actors struggle for dominance. The signs have been around for years. The first major Internet worm attack took place in 1988. Industrial espionage has also moved onto the Internet. Theft, piracy, and con artist scams occur across the Internet despite the fact that most businesses work hard to defend their goods.

Concerns about the need to guard critical infrastructure crested with the release, in 2003, of the National Strategy to Secure Cyberspace. It brought home the fact of US vulnerability and gave a new sense of what is really at stake. Today, several nations are committing significant resources to acquire the capability to mount sophisticated cyber attacks. Indeed, the attacks are going on now. They seek to disrupt US systems across a spectrum of operations. At one end of the spectrum are the annoying hacker intrusions and localized network crashes. At the other end lurks the possibility that a foe could bring catastrophic destruction and failure of military systems or generate illusions to take the place of authentic information.

Over the past 10 years, military information systems have been subject to increasingly relentless cyber attack. Parties are constantly scanning US networks for entry. One defense official recently estimated that someone mounts an attack every eight seconds, on average. Pentagon officials

development. A good many of the most vital capabilities remain classified because of their connection with intelligence gathering and encryption systems.

Threats and opportunities have abounded, but many were skeptical about calling cyberspace a warfighting domain before a war had even broken out there. For all the concern about stepped up attacks and global malware operations, the idea of war in cyberspace remained stuck in the realm of theory. All of that changed utterly on April 26, 2007.

WEB WAR I

On the evening of that day, at about 10 p.m., someone launched a massive, no-warning cyber attack on the Baltic nation of Estonia. In its opening minutes, bursts of electronic messages began to flood Estonian government websites. Firewalls were up, extra servers were ready, and an emergency response team was standing by for just such an eventuality. Yet these defenses were easily breached. The attack count experienced exponential growth. There were about 1,000 assaults on the first day. On the second day, there were 2,000 attacks *per hour*. These denial-of-service attacks quickly forced the Estonian government to shut down several websites—some for hours, some for days. The Parliament’s email server was an early casualty. More waves followed, with the last major incidents recorded on May 18.

DOD photo/Cherie Thurlby



On May 14, 2007, NATO Secretary General Jaap de Hoop Scheffer warned, “No member state is protected from cyber attacks.”

have revealed that a June 2007 attack temporarily disabled unclassified Pentagon office computer systems as well as the e-mail system in the Office of the Secretary of Defense.⁴ The United States has not been idle, either. A virtual arsenal of offensive cyberspace weapons is now in various stages of

NATO quickly took notice of this attack on one of its members. “No member state is protected from cyber attacks,” said NATO Secretary General Jaap de Hoop Scheffer on May 14, 2007. US officials were similarly alarmed. “Russia, our Cold War nemesis, seems to have been the first to engage in cyber warfare,” warned Secretary of the Air Force Wynne. He called the Estonian events “the first known incidents of such an assault on a state.”⁵ At a June 2007 NATO meeting, the American Secretary of Defense, Robert Gates, urged his fellow defense ministers to begin planning how they would respond to a cyber attack.⁶

“If a bank or an airport is hit by a missile, it is easy to say that is an act of war,” said Madis Mikko, a spokesman for the

4. Demetri Sevastopulo and Richard McGregor, “Chinese Military Hacked Into Pentagon,” *Financial Times*, Sept. 4, 2007.

5. A.J. Bosker, “SECAF: Dominance in cyberspace is not optional,” Offutt AFB, 55th Wing Public Affairs, May 31, 2007.

6. Greg Jaffe, “Gates Urges NATO Ministers to Defend Against Cyber Attacks,” *Wall Street Journal*, June 15, 2007.



Left: AP/NIPA, Timur Nisanotdinov. Right: AP photo

Left, ethnic Russians protest in front of “the Bronze Soldier,” the proposed relocation of which sparked the Estonian crisis. Right: Estonian police in riot gear disperse a demonstration in downtown Tallinn.

Estonian defense ministry, adding, “But if the same result is caused by a cyber attack, what do you call that?”⁷ Estonian Minister of Defense Jaak Aaviksoo had a description for it. At an international conference in Paris in June, he called what had just happened “the unnoticed third world war.”⁸

At the center of the Estonian crisis lay an only too tangible object—something called “the Bronze Soldier.” It was a sculpture, in bronze, of a World War II Soviet soldier, his bare head slightly bowed in memory of fallen comrades. Nazi German troops occupied the Baltic state from 1941 through 1944. Soviet forces ejected them and retook the capital, Tallinn, in October 1944. The statue commemorated the sacrifice of the Soviet troops and served as a positive symbol for Estonia’s minority ethnic Russians, bereft after the Soviet Union collapsed and Estonia reasserted its independence.

For many ethnic Estonians, however, the statue was nothing less than a constant reminder of long years of postwar Soviet occupation and oppression. The Reform Party, having won the Estonian elections of March 2007, promised to relocate the Bronze Soldier to a less sensitive site and set a date for the move. As the date for the dismantling approached, street riots broke out.

Certainly, the leaders of Estonia were fully aware of the possibility of cyber attacks. “If there are fights on the street, there are going to be fights on the Internet,”

said Hillar Aareleid, Estonia’s director of computer emergency response.⁹ The danger was clear because Estonia is one of the most fully wired societies in Europe. Use of the Internet had become a deep, daily feature of life for many. The World Bank ranked Estonia’s preoccupation with the net as being just behind that of the United States and well ahead of 15 older members of the Western Alliance.

Estonians were also angling to turn their cyber stance into an edge within the NATO framework. In December 2006, Tallinn suggested that NATO should set up a cyber defense center in Estonia. “The aim of the center would be to promote cooperation between NATO members on cyber defense, draft training programs, and deal with the legal aspects of fighting cyber terrorism,” said Lauri Allmann, a top official in the Estonian Defense Ministry.¹⁰ Alliance officials had taken the proposal under advisement.

For all that, Estonia was ill prepared for an assault of the scale, intensity, and duration that was seen in Spring 2007. The magnitude of the attack is underscored by the recitation of a few basic facts:

- On May 9, the peak day of the attack, Estonian networks were hit every second with an average of four million packets of data, a huge amount.
- Targets rose to the hundreds, ranging from government sites and banks to newspapers and universities.

7. Christopher Rhoads, “Cyber Attack Vexes Estonia, Poses Debate,” *Wall Street Journal*, May 18, 2007.

8. Estonian Ministry of Defense news release, “Internet: XXI Century battlefield,” June 16, 2007.

9. Mark Landler and John Markoff, “Digital Fears Emerge After Data siege in Estonia,” *New York Times*, May 29, 2007.

10. “Estonia Offers NATO Cyberdefense,” *IOL Technology*, Dec. 8, 2006.



point, the attackers pushed forward a single, massive data burst designed to measure the capacity of the network. Hours later, multiple computers launched massive bursts that hit the network with hurricane force and incapacitated the Estonian routers.

The street riots stopped on April 29, but the cyber assaults, which had already lasted for three days, went on with no letup. On April 30, daily newspaper sites went down. Estonia, by now in full emergency mode, tried to fight back. In 2006, Estonia had established a Computer Emergency Response Team (CERT) with assistance from the European Network Information Security Agency; it went into full swing.

The Estonian Minister of Defense, Jaak Aaviksoo, warned that the West had embarked upon “the unnoticed third world war.”

Moreover, NATO experts were sent to help. By May 2, Internet service providers around the world had fully mobilized and were doing all they could do to assist, following long-standing practice for countering viruses and worms.

Still, these measures weren't powerful enough to halt the attacks. "The cyberattacks against government websites have come in waves," said Hillar Aarelaid, head of Estonia's CERT, and added, "They start and end, and then start again."¹¹

On May 9-10, executives at Hansabank, the largest financial institution in Estonia, made the hard decision to take the enterprise offline. The attacks had made it too dangerous to stay connected. The bank shut down all service for an hour and a half and then closed all services to customers outside the Baltic states. "The nature of the latest attacks is very different," Linnar Viik, an Estonian government IT consultant, said of the Hansabank penetration. "It's no longer a bunch of zombie computers"¹²

Officials hoped the Hansabank attack would prove to be the last stage of the attack, but they were wrong. On May 15, renewed assaults struck Estonia's second-largest bank, the Swedish-owned SEB Eesti Uhispank. According to a bank spokesman, Silver Vohu, the financial establishment came under "massive attacks" and was forced to keep computers outside of Estonia from gaining access to its online banking service.¹³ "It turned out to be a national security situation,"

■ Attacks were carried out by amateurs and by highly skilled cyber attack specialists with significant resources.

■ The computer attacks on Estonian were vectored in from more than 50 countries. Many attacking computers had been co-opted by operators in other countries.

The attackers used straightforward denial-of-service tactics. This method of attack had been seen before. It seeks to send forward data requests and overwhelm a particular router's capacity, paralyzing the highly specialized computers responsible for selecting a path and forwarding information packets. Routers are the critical links between a network (such as that used by the Estonian parliament) and the Internet. The attackers also used illicitly linked computers around the globe to mount an enhanced onslaught. These attacks were conducted by networks of "bots"—a bot being an automated program that accesses web sites and then traverses the site by following links on its pages. Bots typically have some form of artificial intelligence and carry out tasks in lieu of a real person. Hackers invisibly take over some functions of computers somewhere in the world and then deploy them for coordinated, simultaneous attacks.

The Estonian attacks were carefully calibrated. At one

11. "Estonia Sees Red in Cyberattacks," *IOL Technology*, May 16, 2007.

12. Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post*, May 19, 2007.

13. "Cyber Attacks Force Estonian Bank to Close Website," *Agence France Presse*, May 16, 2007.

defense minister Aaviksoo said. “It can effectively be compared to when your ports are shut to the sea.”¹⁴

RUSSIAN FINGERPRINTS?

In retrospect, it was clear that Estonia was highly vulnerable to such an assault. Overwhelming Internet dependence was one problem; Estonia’s Internet usage had expanded dramatically after 2000, as was the case in many countries around the world. By 2007, almost 52 percent of Estonia’s population of 1.3 million had Internet access. More worrisome was Estonians’ dependence on the Internet. According to the Defense Ministry, 60 percent of Estonians used the Internet every day, and a full 97 percent of banking transactions took place online. Internet-based government systems figured in the everyday conveniences of Estonians. For example, Estonians used cell phone Internet connections to pay for street parking. They also voted over the Internet and used it to pay taxes. Being such a “wired” society was seen as a major economic edge for the small nation.

Estonia also clearly had a big and highly sophisticated enemy out there. Aaviksoo, the defense minister, declared that it was “a politically motivated offensive cyber campaign.”¹⁵ Indeed, the attack against Estonia stood out as being a calculated and carefully planned event. First, there was a wide range of targets. Second, the attackers had the clear capability to strike a sustained series of painful blows during a brewing crisis. Third, it was clearly an attack on the Estonian state and major institutions, from the press to the banks. Fourth, the attackers achieved several hard-to-reach goals, from shut downs and major disruptions of critical government sites to the posting of false messages on sites presumed to be authentic.

For several years, security experts had predicted that a computer network attack would prove to be a weapon of mass effect and damage. “While primarily a technical means, successful CNA depends upon clear intelligence, well-defined intent, and clear understanding of the primary and secondary effects of an operation,” wrote William J. Bayles in the Spring 2001 issue of the military journal, *Parameters*.¹⁶ Estonia’s attackers seemingly calculated all that in advance.

Because it had motive, means, and opportunity, Russia

was widely viewed as the main suspect in these attacks. Left hanging, however, was firm attribution of who was responsible for the cyber attacks. Russian-backed groups had clearly been involved in some phases of the Bronze Soldier conflict. For example, Russians in Moscow constantly harassed Estonia’s ambassador in the capital city. A Kremlin-funded youth group called Nashi also shut down the main highway between Russia and Estonia.¹⁷ From the political perspective, there was no question about Russia’s displeasure with Estonia. Russian embassy officials, in a formal statement early in the crisis, declared it “unacceptable” to dismantle and move the statue and attempt to “rewrite history in order to win points in domestic politics.”¹⁸

Some of the cyber fingerprints also suggested Russian involvement. Estonian government sources found Russian government Internet addresses among the traces left by the attacks. “There are strong indications of Russian state involvement,” said Silver Meikar, a member of Estonia’s Parliament, who based his claim on “a wide range of conversations with people in the security agencies.”¹⁹ Still, the nature of cyber attack made the charges hard to verify. Russia officially denied involvement, and pointed out that, while some Russian Internet accounts were implicated in the attack, Russian computers could have easily been used by hackers outside of Russia itself.

As the Estonians ultimately characterized the attack, many participants from amateur to professional could have taken part. The political controversy surrounding the Bronze Soldier was certainly capable of drawing a large number of attackers, inside and outside Russia. However, in late summer 2007, there was a kind of break in the Estonian case. An investigative journalist cooperating with Internet security firm Arbor Networks uncovered great similarities between the Estonian botnet attack and a previously known Russian assault against opposition parties led by Garry Kasparov, the Russian international chess champion and critic of the Putin regime. Arbor Networks confirmed that there was significant technical and procedural overlap between the Kasparaov attacks and the Estonia attacks. The botnet “signature” provided firmer evidence of Russian involvement, perhaps even the active involvement of a special branch of

14. Mark Landler and John Markoff, “Digital Fears Emerge After Data Siege in Estonia,” *New York Times*, May 29, 2007.

15. Jaak Aaviksoo, Estonian Minister of Defense, “Cyber Defense—The Unnoticed Third World War,” Address to the 24th International Workshop on Global Security, Paris, June 16, 2007.

16. William J. Bayles, “The Ethics of Computer Network Attack,” *Parameters*, Spring 2001.

17. Owen Matthews and Anna Nemtsova, “Putin’s Shock Forces,” *Newsweek*, May 28, 2007.

18. “Estonia Reburies Soldiers Despite Russian Protests,” *Deutsche Welle*, July 3, 2007.

19. Peter Finn, “Cyber assaults on Estonia Typify a New Battle Tactic,” *Washington Post*, May 19, 2007.

the Federal Security Services, the successor to the infamous KGB.²⁰

“PERFECT BATTLEFIELD”

The frustration of this kind of cyber “manhunt” is an all too common feature of cyberwar. For developed states, the cyber attacks on Estonia also marked the undeniable arrival of a major new worry. “Estonia is the first example of a situation where the threat was real, not imagined; NATO must take it very seriously,” noted Poland’s defense minister, Alexander Szczyklo, in a June 12 statement. Cyber defense also made the agenda for NATO’s June 2007 ministerial session.²¹

For NATO, the Estonian incident raised important questions about how to define the type of cyber attacks that might become actionable under Article 5 of the Atlantic Treaty. That “mutual defense” clause calls on each and every member to treat an armed attack on any NATO member as an attack on itself and to take action in defense of the threatened party. NATO did send netwar experts to Estonia to provide assistance, but that feel far short of Article 5 seriousness. “We haven’t yet defined what can be considered to be a cyberattack, or what are the rights of member states and the obligations of EU and NATO in the event such attacks are launched,” Aaviksoo said.²² He continued: “The EU and NATO need to work out a common legal basis to deal with

Because Estonia was a small, heavily wired state, the cyberattacks painted a realistic picture of a true cyber threat to national security. “In the 21st century, ... a state is no longer only its territory and its airspace, but it’s also its electronic infrastructure,” said Viik, the Estonian government cyber specialist.²⁴ Defense Minister Aaviksoo summed up the problem in a June address to a security conference in Paris. “In essence,” he said, “cyber attacks against Estonia demonstrated that [the] Internet already is a perfect battlefield of the 21st century. In Estonia’s case, effective political propaganda can motivate a significant number of people to launch a massive cyber attack almost instantly.”²⁵ The impact on Estonia was substantial because of its heavy reliance on the cyber domain.

Aaviksoo then made several trenchant points. First he argued for “acknowledging the impact of cyber defense on our civilian as well as military affairs.” Second, he pointed to Estonia’s “transparency and eagerness to cooperate” with others as reasons it was able to mobilize quickly and minimize the damage. Next, he said, “when tackling a problem that is international in nature such as cyber defense, more rather than less cooperation is the only way to deal with it.”

Members of the pro-Kremlin and anti-Estonian youth group Nashi block a gateway that was to be used by Estonia’s ambassador to Moscow. Nashi also blocked the main Estonia-Russia roadway.

cyberattacks. For example, we have to agree on how to tackle different levels of criminal cyber-activities, depending on whether what we are dealing with is vandalism, cyberterror or cyberwar.”

Senior US defense officials also expressed concern and acknowledged the uncertainty following the June 2007 NATO meetings. “If a full-on [cyber] attack cripples an electric grid or shuts down a country’s oil fields or something like that, does that constitute an Article 5 attack?” wondered one US defense official, adding, “When NATO planners do their review, that is something that they will have to take into consideration.”²³



AP photo/Mikhail Metzel

Cyberspace defense “will not work if there are national or international judicial gaps,” he added. The Estonian defense minister, who had just seen cyberwar up close and personal, conceded that he did not have many answers to the major

20. Joshua Davis, “Hackers Take Down the Most Wired Country in Europe,” *Wired*, Sept. 15, 2007.

21. Estonian Ministry of Defense news releases: “Minister of Defense meets Finnish counterpart,” May 6, 2007 and “Minster of Defense discusses cyberdefense with his Polish counterpart,” June 12, 2007.

22. “Estonia Sees Red in Cyberattacks,” *IOL Technology*, May 16, 2007.

23. Greg Jaffe, “Gates Urges NATO Ministers to Defend Against Cyber Attacks,” *Wall Street Journal*, June 15, 2007.

24. Peter Finn, “Cyber Assaults on Estonia Typify a New Battle Tactic,” *Washington Post*, May 19, 2007.

25. Jaak Aaviksoo, Estonian Minister of Defense, “Cyber Defense—The Unnoticed Third World War,” Address to the 24th International Workshop on Global Security, Paris, June 16, 2007.

questions. Then he warned, “I fear that, if we do not start answering these hard questions soon, we will not be able to deal with the future effectively.”

Some experts pointed out that, from a technical

USAF photo/TSgt. Cohen Young



Secretary of the Air Force Michael Wynne was instrumental in declaring cyberspace to be a new Air Force operational domain, on a par with “air” and “space.”

standpoint, the denial-of-service attacks that dominated the Estonian affair did not even represent a very high level of cyber sophistication. Other nations, the US included, had suffered similar, if shorter, disruptions at the hands of talented, but isolated, hackers. Still, the orchestrated and provocative nature of the attacks put the Estonia cyberwar in a new category. Part of the shock of the Estonian affair was that it transformed cyberspace, once and for all, into an area of state conflict. The world now had entered an era in which states attacked states in their cyber territories. The fact that the attacks could not decisively be pinned on Russia or on any particular group of attackers stoked fears that Internet attacks could not be deterred and might well spiral out of control.

“Estonia was kind of a wake-up call,” summed up Cartwright in September 2007. Estonia was “point-defended at the computer firewall” as Cartwright described it.²⁶ When “the scale of activity exceeds what their situation awareness can handle, then they find themselves in extremis and probably without the tools to control it.”

“We’ve got to make sure we have situation awareness at a scale commensurate with our equities,” Cartwright concluded.

THEATERS OF CYBERSPACE

As the Estonia example demonstrates, America faces a hugely complicated problem when it comes to the subject of conflict in cyberspace. Combat in the cyber domain not only

could take place in many different forms and be launched in many different ways but also unfold across different theaters of operations. Currently, there are two such theaters.

First, there is the commercial Internet. America’s Internet dependence has emerged as a point of vulnerability—as USSTRATCOM has pointed out. The Estonia attacks were a chilling example of what can happen if a determined foe wishes to take advantage of that vulnerability. Second, there are the secure and classified military networks that branch

out across the electromagnetic spectrum. The United States over the past decade has entrusted more and more of its warfighting “valuables” to these networks, seeking an edge through fast communications and rapid information transfer. The Air Force is the leader in US military cyberspace. The challenge for the Air Force is to protect and extend its cyberspace functions.

Understanding cyberwar—and the rise of cyberspace as a warfighting domain—requires discussion of both of these theaters of operation. The roots of cyberwar go back to concepts of the 1960s, with some smaller offshoots going back even earlier in the Twentieth Century. As it turns out, the histories of the civilian Internet and military cyberspace run in parallel, and then diverge, only to meet again at key moments in recent history.

What is clear beyond any doubt is that cyberspace, as it exists today, contains lots and lots of military DNA. It was not clear for a long time whether cyberspace would become a distinct warfighting domain. It was conceived originally as a functional community network to make it easier and quicker for researchers to work together. For nearly two decades, it grew from West Coast experiment to worldwide phenomenon with few hints of its full potential—or its vulnerability. Only much later did both become fully apparent.

The Defense Department’s Advanced Research Projects Agency was perhaps the main source of invention and implementation of “packet switching,” the basic concept underlying creation of wide area networks to form the early Internet. The process breaks down electronic messages into finite-size “packets” of data that will always be accepted by a network. These message bits zoom out over many different

26. Author interview, Gen. James E. Cartwright, vice chairman, Joint Chiefs of Staff, Sept. 14, 2007.



Research Projects Agency) to create and implement the TCP/IP standard, which defined the first true Internet in 1983. European networks connected in the 1980s. In 1991, China hosted its first TCP/IP connection.

By that time, however, the US had experienced a kind of schism in cyberspace. The military had split away and gone off on its own in 1983, when the Internet was still a collage of separate networks. The result was the MILNET, a collection of US military users that retained only a few connections to the other, wider, civilian network. In the 1980s, there emerged a separate Defense Data Network emerged, handling traffic at different levels of security. The DDN

Gen. Michael Moseley, the Air Force Chief of Staff, was the air boss of Operation Iraqi Freedom in 2003, when the US mounted a well-defined military campaign in cyberspace.

ceased operation in 1995, replaced by several new networks. New routers supported what became the Nonsecure Internet Protocol Router Network (or NIPRnet), Secure Internet Protocol Router Network (SIPRnet) and the Joint Worldwide Intelligence Communications System (JWICS). NIPRnet, SIPRnet, and JWICS are still around today.

Meanwhile, in the civilian side, commercial pressure drove business networks forward to merge with efforts of universities and research institutions. The end result? Today's Internet, a truly global network connected to massive commercial databases housing significant intellectual capital and commercial equities. In the words of Cartwright: "It's the nervous system of our country."²⁷

American business began heavy reliance on computers in the 1950s but development of a network was slower in coming. Aside from the early users of ARPAnet and its cousins, few businesses had the ability to connect. However, that changed in the latter decades of the 20th century. Inexpensive desktop computers with interoperable software and browsers for the Internet revolutionized business landscapes in the 1990s. Netscape Version 1.0 appeared in December 1994. Windows 1.0 followed in August 1995 and Windows 2.0 went final in November 1995. Now in place were all of the pieces required to support commercial computer networking, which would change global business.

TROUBLE IN PARADISE

There was, however, a huge problem on the horizon. As was evident to anyone who cared to look, the adolescent

circuit paths. At the ends of these circuits, at a destination, packets arrive and are reassembled, creating an intact message or file.

After discussions among computer researchers in the late 1960s, ARPA in 1969 awarded a contract to develop the so-called "ARPAnet." ARPA, by the end of that year, had lashed together a rudimentary network linking four nodes at four universities—UCLA, Cal-Berkley, Stanford, and Utah. E-mail became common on the net in the early 1970s. More universities and research institutions connected until there were 57 Internet message providers by 1975. ARPA turned the contract over to the Defense Communications Agency that same year. It took advances and standardization of protocols (some funded by the renamed Defense Advanced

27. Gen. James E. Cartwright, commander, US Strategic Command, testimony, House Armed Services Committee, March 8, 2007.

Internet was a security nightmare. Most of the major threats in the world of cyberspace began well outside the military networks. Primitive forms of worms and viruses were detected in the ARPANet and other early networks. However, it was not until these networks achieved a degree of national and intercontinental linkage that so-called malicious programs, or “malware,” had the opportunity to cause widespread and serious trouble.

When that happened, though, trouble was soon in coming. In the late night hours of Nov. 2, 1988, students working on the Internet began to notice an unusual slowing and disruption of service. Around midnight, a Harvard student posted an anxious message, saying, “There may be a virus loose on the Internet.” In a post-mortem conducted seven years after this historic event, Charles Schmidt and Tom Darby, described the scene in this way: “The Internet was coming apart. VAX and Sun machines across the country were being overloaded by invisible tasks, preventing users from being able to use the machines effectively, if at all, and eventually forcing system administrators to cut off many of their machines from the Internet entirely in an attempt to cut off the source of infection.”²⁸

The culprit, as is now well known, was the “Morris Worm”—a nasty little bug named after its creator, 23-year old Cornell University graduate student Robert Tappan Morris.

Cornell University student Robert Morris Jr., creator of the infamous 1988 “Morris Worm,” leaves federal court. He was found guilty of computer tampering laws.

Morris had managed to gain entry to a Harvard-based computer and used it to launch the worm code, the better to conceal his identity. The young Internet was vulnerable to such an attack because it had been built for speed and convenience, not security; its ethos was to bring more users aboard, not lock them out. The situation was perfect for a mischief-maker like Morris. His worm propagated rapidly and hampered operations of 60,000 computers across the nation. It exploited UNIX code designed for convenience, and it took advantage of the fact that security was an afterthought to users who wanted functionality—period.

Morris’s creation is regarded by most as the first truly noteworthy malicious software, but Morris didn’t invent malware; the earliest worms appeared in the 1970s and 1980s. It appears that some actually began as beneficial maintenance programs. However, the independent and self-sustaining

nature of worm codes had a destructive side, which became evident to all. The Morris Worm was, in reality, a prank, a self-replicating computer program that harmed the network by making copies of itself and sending them to many other addresses, consuming bandwidth and clogging up the cyber roadway. Today’s hackers do far more damage with far more sophisticated programs. No one is more aware of this than Morris himself; two decades after he sent his famous worm into the world, he is a tenured computer science professor, working at the Massachusetts Institute of Technology in Boston.

Schmidt and Darby, authors of the Morris Worm study, regarded the year 1988 as a kind of watershed time. “Before late 1988,” they noted, “computer security was not a major concern of the Internet community.” Afterward—at least, after Nov. 2—it was. Yet the vulnerability itself had been there all along. Malicious codes found weak spots in systems



AP photo/Michael J. Okoniewski

built in a rush. The Morris Worm, for example, did its work by creating buffer overflow—creating an amount of data beyond what the system was designed to handle. There were no barriers to this. Attempts to accommodate the buffer overflow led to system breakdown.

Worms were included in one category of cyberspace “weapons” consisting of malicious code targeted to disrupt network systems and functions. Worms may impair functionality by spreading, as the Morris worm did. Worms can also contain a payload consisting of execution instructions, such as deleting files. Botnets are created by worms carrying a payload that opens a “backdoor” to a computer, making it into a zombie controlled by outsiders.

28. Charles Schmidt and Tom Darby, “The What, Why, and How of the 1988 Internet Worm,” www.snowplow.org.

Also detected frequently on the Internet in the mid-1980s were viruses. In fact, the first simple ones were seen on ARPAnet in the 1970s. Unlike a worm, a virus infects and corrupts good and functional files. Most viruses have to be opened from an attachment or another source, such as an infected computer disk. At first, viruses spread via such removable disks. Then “viruses in the wild” began to spread through networks. One of the first was a boot sector virus named Brain, written by two Pakistani software developers seeking to punish, and thus deter, commercial pirates who were getting rich making illegal copies of their software. Others wrote macro viruses to attack Microsoft office software. As Microsoft’s market share burgeoned in the 1990s, it became easier for such a virus to strike a huge share of the world’s software.

The lackadaisical attitude toward computer security was nothing less than an invitation to trouble. Malicious code typically used Internet connections to crack weak spots in operating systems. New systems could open up the possibilities for new worms. The race was on.

HACKERS AND CRACKERS

By the late 1990s, attacks on commercial and government sites had grown and changed in character. The first generation of hackers and crackers were computer scientists or aficionados pushing the envelope. Gaining access to formerly inaccessible areas was the major payoff.

However, there quickly followed a second generation of for-profit operators. Next came industrial spies and thieves. “The hacker today isn’t just the stereotypical computer geek with a grudge against the world because he can’t get a date,” opined James Adams, the CEO of the private Infrastructure Defense, Inc., during March 2000 testimony before the Senate Committee on Governmental Affairs. He added, “The hacker today is much more likely to be in the employ of a government, big business, or organized crime.” As companies entrusted more proprietary goods to databases, there arose a market for breaking into them and stealing plans for the latest products. Cracking the database and downloading the

goods worked just as well as breaking into a physical factory office. Highly talented “black hats,” adept at these kinds of operations, were scattered around the world.

“Targeted sites receive hits on their servers of up to one gigabyte of data per second, and are unavailable to the general public for anywhere from 30 minutes to several hours,” Adams told the Senate panel. Yahoo, eBay, Amazon, Microsoft, E*Trade—the biggest names in online business were among the favorite targets.

Even so, Internet usage mushroomed, becoming a medium of multiple and critical tasks. From 2000 to 2007, the sheer number of Internet users became an important factor. It grew by more than 200 percent globally, topping out at some 1.1 billion persons worldwide.²⁹ In the first years of the 21st century, the spread of Internet usage and the proliferation of tasks turned cyberspace into a distinct operational domain. Security measures increased, too.

If three decades of experience suggests anything, however, it is that cyberspace, with its multitude of commercial and other public applications, simply can’t be completely secured. The “National Security Strategy to Secure Cyberspace,” released in February 2003, identified a vast number of computer security weak spots. It said that it actually found significant growth in the number of faults in software and hardware that could “permit unauthorized network access or allow an attacker to cause network damage.” The number of faults in 2000 was 1,090. In 2002, it was 4,129.

Harmful events continued to erupt on the net. In August 2005, two young Moroccans were arrested on a charge that they had encoded and released the Zotob Worm. This worm again used buffer overflow to target a specific vulnerability in Microsoft systems. The Zotob Worm was notable because

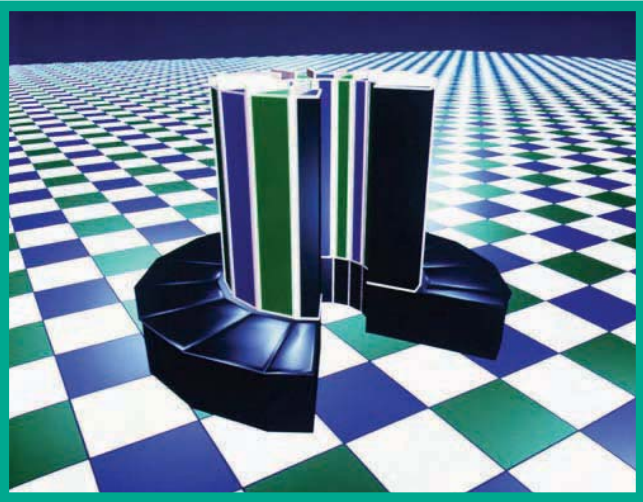
Lt. Gen. Robert Elder Jr. (right) led the USAF cyberspace effort as 8th Air Force commander. Here, he meets USMC Gen. James Cartwright, then commander of US Strategic Command and now vice chairman of the Joint Chiefs of Staff.



USAF photo/SrA. Sonya Padilla

29. Internetworldstats.com.

Cray, Inc. image



attacks would actually prove to be. Anti-virus software had to an extent begun to inoculate home desktops and business systems. Internet service providers became adept at blocking many efforts to take down operations and at restoring critical functions when such efforts did succeed. Corporate America

A “self-portrait” created by a Cray 1 supercomputer. Massive Cray computers were integral to systems used by Strategic Air Command in the 1970s.

it infected two major television enterprises—ABC and CNN—as well as the Department of Homeland Security. It also shut down operations of some firms in Germany and Asia. Microsoft mobilized two “war rooms” and urged users to download a security patch to halt the worm.³⁰

The big boys also showed up. That same month, August 2005, also featured the first public disclosures of Titan Rain, a major and systematic attack on Department of Defense systems that seemed to originate in China. Reports suggested that high-skill attackers since no later than 2003 had been breaching government sites such as Sandia National Laboratories and private networks at corporations such as Lockheed Martin. The attackers sought to steal sensitive material from computer hard drives and to create botnets for future cyber operations. One specialist was reported to have found that a particular series of attacks originated from three routers in the Chinese province of Guangdong.³¹

The rise of cyberspace had a far-reaching impact. For perhaps the first time since the Industrial Revolution, major new weapons of war were coming not only from state-based militaries or insurgent gangs but also from private citizens. The Internet was built with extensive government support from many countries, but its black hats seemingly sprang from nowhere. The typical cracker profile was a young male aged 16 to 25, sometimes acting with financial backing. The territory they sought to control for pride or profit was cyberspace. The 20-year progression of the Internet had led to the production of a formidable arsenal of worms, viruses, denial of service bots, and other forms of attack.

Still, debate continued over just how serious Internet

felt the sting of having to pay protection money, so to speak. Still, the sum total of the first 20 years of Internet attacks caused barely a ripple upon the smooth and glassy surface of this glamorous new technology.

Estonia changed the paradigm by providing a case where, at least according to national officials, the pain was real. Estonia had to seal its cyber borders and government officials and the public alike experienced disruption. After Estonia, it was easy to see that multiple, sustained cyber campaigns could create mayhem on the scale of a natural disaster.

MILITARY TERRITORY

For the denizens of military cyberspace, the headline event was not Estonia. The big step had been taken four years earlier, at the start of Operation Iraqi Freedom in March 2003.

Military cyberspace, as we have seen, is not the same as Internet cyberspace. True, the Internet is sometimes part of the military picture; it can serve as a transport layer—a system on which military messages travel—and, adversaries assume, as an avenue of American attack. However, the Air Force’s major systems of warfighting cyberspace are distinct from the Internet. “The Internet, from a warfighting standpoint, really has no piece to it,” Elder told the author in a July 2007 interview. That’s because the same quarter-century that gave rise to the global Internet also produced a very different realm of military cyberspace. In this, some of the most critical developments were conceived and led by airmen.

It must be said that the development of ways to conduct warfare in cyberspace actually got off to a slow start. This is not to be confused with use of computers. Computers began making major contributions to military operations as far back as World War II. Systems integration projects in the 1950s pushed the concepts further in support of advanced

30. “Worm Strikes Down Windows 2000 Systems,” CNN.com, Aug. 17, 2005.

31. Nathan Thornburgh, “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),” *Time*, Aug. 29, 2005.

weapon systems. For much of the Cold War, massive Cray computers were integral to the systems used by Strategic Air Command for attack warning and operations. Combat over the electromagnetic spectrum emerged in World War II and continued ever after. Radar games and signals intelligence were two examples.

Still, the constitution of cyberspace had not occurred in the military world any more than it had in the civilian business sector. There was no architecture, no network, and no electronic commerce to speak of. At first, military systems were driven by many of the same technological innovations that led to creation of the Internet. After they split from ARPAnet in 1983, the military Internet systems took quite a different route into the future. Secure networks were established rapidly, but, in their early forms, these systems did not permeate military operations. In fact, the military was not significantly changed until it came face to face with the same potent combination of Internet technologies, cheap desktop computers, and flexible software that changed commercial practices. Then three things happened. First, airmen developed battlespace networks that moved beyond the platform. Second, the Pentagon embraced the concept of net-centered operations as a way to transform warfare. Third, the Bush Administration decided on war in Iraq.

In the 1990s, US military cyber power progressed from a limited, intelligence-based capability to an actual warfighting instrument. Americans were welcoming the Internet into their daily lives. At the same time, the Air Force was employing its own tactical and operational cyber networks to reach new peaks of combat performance. These networks became the skeletal structure of cyberspace as a warfighting domain.

For airmen, the major conceptual hurdle to overcome was a long-held belief that all of the critical work, whatever it was, had to be done on the aircraft itself. “Before, there was always a C4ISR enabler,” Elder observed. “The Air Force bought systems without thinking through the cyber implications. At the time, everything was done on the plane.” However, new datalinks and secure command and control arrangements opened up a robust, wide area network of information that could reshape air attack. Then, two big changes occurred.

First, command and control networks based upon the air operations center greatly expanded, creating real-time, globe-spanning reach for airmen everywhere. Elder noted that it took five months—the period known as Operation Desert Shield—to get Coalition information resources in order. “The hold up was not deploying more forces,” Elder asserted. “The hold up was really command and control.” Ten years later, Operation Enduring Freedom suffered far less delay. The coalition had immediate options, “thanks

largely to satellites we could go anywhere in the theater with same connections as in the United States,” Elder added.

Second, operators generated new airborne networks, mini-cyber domains in the battlespace dedicated to specific tasks. In effect, these operators organized their corner of cyberspace and the electromagnetic spectrum into a wide area but limited access network which provided new warfighting capability, usually at the tactical or operational level. One example was Link 16. The NATO-standard Link 16 datalink allowed users to create a network of aircraft and ground stations within line of sight restrictions (with some recent extensions for longer reach protocols.) With Link 16, members of the net could pass voice communications, send data (at a limited rate), or transfer imagery. Link 16 organized a tactical picture shared by multiple users in near-real time.

Was this new combination of air operations centers and tactical nets based on Link 16 really so different? Command and control networks and airborne networks had been around since the spread of radios in airplanes and were widely used in World War II. However, the new networks of the 1990s began to open up much greater functionality, extending communications ranges and enabling rapid transmission and storage of data, which eventually included images and video. The Air Force moved to incorporate computers and more fully automate air operations centers, based on the Theater Battle Management Core Systems element and other types of foundational arrangements.

The real change came when these networks allowed airmen to strike not only preplanned targets but also unplanned, “emerging” targets that might pop up unexpectedly in a battlespace. Granted, the air commanders of Desert Storm had only limited power to redirect airborne aircraft to new targets, but that had changed by the start of Operation Allied Force over Serbia in March 1999. Declaring “the air operations center is a weapon system,” airmen learned to exchange, integrate, and act on information more quickly than had been true even in the Gulf War.

The 1999 air war over Serbia became a beta-test version of network centric warfare. During a 78-day air campaign, networked air operations centers connected to digital datalinks empowered commanders to send new target coordinates to aircraft in flight. In one such case, a Navy Tomahawk land-attack cruise missile was retargeted to strike a parked Serbian MiG-29. Computer simulation and modeling was used to predict movements of Serbian surface-to-air missile batteries. Numerous fighters and bombers were retargeted while airborne. None of it could have happened without the newfound US mastery of the cyberspace domain.

By the start of OEF in Afghanistan on Oct. 7, 2001, the pilots of most USAF and Navy aircraft took off with expectations that they be redirected to new targets while airborne. That was a marker of a greatly enhanced battlespace network. For many defense officials, it was also a wake-up call about the importance of cyberspace and the need to dominate it in the face of all adversaries.

proliferation of information technologies will substantially change the conduct of military operations.”

What happened between JV 2010 and JV 2020?

In reality, very little had changed with respect to the tactical prowess of the Air Force or any other uniformed American service. A far more important factor was a rush of academic theorizing about cyber conflict. Helping to kick off the upsurge of comment was “Cyberwar is Coming!”—a journal article researched and written by John Arquilla and David Ronfeldt of RAND. This early work (it was published in 1993, before JV 2010, but had a delayed impact) was a classic. It was steeped in military history and evaluated the impact of a rapid and distributed information flow. It also attempted to assess how swift data movement would affect military tactics. Arquilla and Ronfeldt believed the information revolution was altering the nature of conflict. Cyberwar implied that communications and intelligence would “develop as adjuncts to overall military strategy” and likely would have “overarching effects that necessitate substantial modifications to military organization and force posture.”

In the Arquilla-Ronfeldt conception of cyberwar, the Air Force was cast in a starring role. The United States, when faced with a regional foe, would use air attacks to eliminate the aggressor’s communications and logistics. “It seems clear that a cyberwar doctrine will give its able practitioner the capability to defeat conventional regional aggression between nation states decisively, at low cost in blood and treasure,” they concluded,

Top: Two airmen update antivirus software at Air Force Cyber Command (P), Barksdale AFB, La. Bottom: The Global Cyberspace Integration Center at Langley AFB, Va.

though they conceded that unconventional adversaries might be harder to overcome. At any rate, the Arquilla-Ronfeldt scheme of cyberwar tended to obviate any purpose for “an entire field army of 400,000 to 500,000 troops.”

Moreover, though the joint doctrine writers might have lagged behind, other parts of the Pentagon seemed to see in the early 1990s the potential value of cyberwar. By the mid-1990s, some Pentagon officials had begun talking somewhat openly—albeit cryptically—about a powerful array of classified cyberspace weapons under development. Vice Adm. Arthur K. Cebrowski was then serving as director for command, control, and communications for the Joint Staff. He said, “Information warfare must become an important instrument of national policy.”³² Cebrowski in 1995 rated

USAF photo/TSgt. Cecilio Ricardo Jr.



USAF photo/Amelia Donnell



NET-CENTRICITY

In 1995, the Chairman of the Joint Chiefs of Staff, Gen. John Shalikashvili, made public a new post-Cold War warfighting “template” for the armed forces. Called “Joint Vision 2010,” the Shalikashvili paper did not identify network-centric warfare as major new feature in the strategic landscape. Rather, JV 2010 only predicted the rise of a “global simulation network” and called on each theater commander to “tap into this ... network.” Five years later, though, everything changed. The new Chairman, Gen. Hugh Shelton, issued a new warfighting template, “Joint Vision 2020.” This paper declared flatly, “The continued development and

32. “Pentagon Developing Cyberspace Weapons,” *Washington Technology*, June 22, 1995.

the deterrent power of the new cyberweapons on a level “somewhere between nuclear and conventional weapons.”

Much of the conversation focused on the need for new definitions and concepts applicable to the realm of cyberspace. “When can you begin information warfare and intrude in someone’s banking system?” wondered Gen. Ronald Fogleman, the Air Force Chief of Staff, in 1995. Emmett Paige, who was then serving as Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C4I), offered a quip: “We have an offensive capability, but we can’t discuss it. However, you’d feel good if you knew about it.”³³

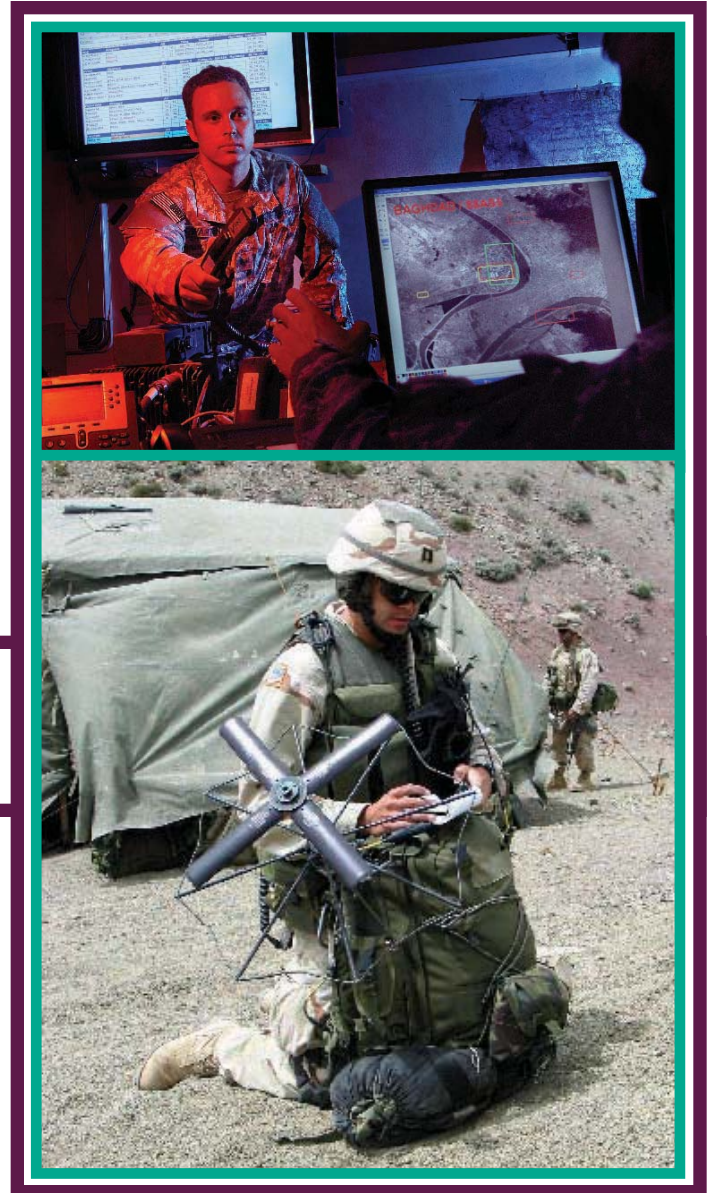
Concern was as prevalent as excitement. Almost as soon as the military networks began to spread, fears about security came to the surface. The Defense Information Systems Agency in 1996 found that the milnets drew as many as 250,000 attacks each year.³⁴ It was at this time—the

Top: Inside the Air Support Operations Center at Camp Victory, Iraq. Bottom: An Air Force air liaison officer talks with an F-16 pilot flying above Afghanistan.

mid-1990s—that initial concepts of netcentric appeared. Cebrowski himself stimulated interest in net-centric warfare while serving on the Joint Staff and stood out as a key advocate for transformational concepts. The impetus came not from his direct observation of military operations but from deep thought about how information technology would change warfare. In this, his model was the business world. As Cebrowski wrote in 1998: “American business has changed. We should be surprised and shocked if America’s military did not.”³⁵

Thus, the enviable inventory systems of Wal-Mart and the data operations of Fortune 500 companies became the main points of departure for the theologians of netcentricity. Comparisons to the emerging information-based economic sectors fed concepts for moving the military from an emphasis on platforms (aircraft, warships, tanks) to an emphasis on the network. From there, it was a relatively short step to worrying about the vulnerability of vital infrastructure of government and private entities.

Military thinking on net-centric warfare came to focus on development of systems and tactics for exploiting the



USAF photo/T.Sgt. Cecilio Ricardo Jr.

USAF photo/Sgt. Russell Wicke

much faster information flow. The Pentagon organized itself around building the five-layered Global Information Grid. Information warfare remained the most frequently used name for all of this effort, and all expected cyberspace to color future warfare. Less popular was the idea of treating cyberspace as a warfighting domain in its own right, but the integration of cyberspace into air and space operations soon made it logical and inevitable.

NETWAR IN IRAQ

It is hard to determine the precise moment in which

33. “Pentagon Developing Cyberspace Weapons,” *Washington Technology*, June 22, 1995.

34. “Computer Attacks at Department of Defense Pose Increasing Risk,” Government Accountability Office, GAO 96-84, 1996.

35. Vice Adm. Arthur K. Cebrowski and John J. Garstka, “Network-Centric Warfare: Its Origin and Future,” *Proceedings*, January 1998.

cyberspace became, for the Air Force, a new and formal domain of military operations. It may have been as early as 1999, with the unfolding of the air war over Serbia. It might have been in 2001, as the United States prosecuted its retaliatory war against al Qaeda in Afghanistan. Certainly, though, it could not have been later than early 2003, the time of the major combat phase of Operation Iraqi Freedom. It stands out as a time in which the US unquestionably mounted a well-defined military cyberspace campaign. After OIF, it was obvious that cyberspace had to be regarded as a new domain.

The first direct hints that cyberspace was destined for bigger things came in July 2002. President George W. Bush signed out National Security Presidential Directive 16, a classified set of guidelines for offensive cyber operations. The directive also reportedly included legal policy on cyberwar. As 2003 began, unofficial reports pointed toward the potential use of cyber attacks in any war with Iraq. A January 2003 symposium at MIT convened 50 experts to discuss cyberwar. They saw cyberspace as a double-edged sword. “There’s a lot of inhibition over doing it,” commented MIT professor Harvey Sapolsky, adding, “A lot of institutions and people are worried about becoming subject to the same kinds of attack in reverse.”³⁶

As UN and military activity signaled the approach of war, experts began to make predictions not just about air strikes and ground invasions but also about cyber operations. In the Feb. 7, 2003 edition of the *Washington Post*, journalist Bradley Graham reported details of the signing of NSPD 16. By March, the level of speculation about cyber ops was at fever pitch. “They’ll use this whole thing as a big training ground,” opined intelligence commentator James Bamford. “They’ll experiment with everything they’ve been thinking about for a long time.”³⁷ An unnamed Bush Administration official assured the *Post*’s Graham, “Whatever might happen in Iraq, you can be assured that all the appropriate approval mechanisms for cyber-operations would be followed.”³⁸

The actual role of cyberspace in the Iraq war was both more muted and more far-reaching than prewar speculation suggested.

Depriving the Iraqi military and political leadership of their “network” and communications abilities was a goal

of the coalition’s attacks. The air component attacked 116 C4I targets as part of what it termed “information warfare physical attack.” Ten media outlets were included among the 116 targets. This represented only about one percent of the total air effort—about the same as the 113 maritime targets on the list.³⁹

However, coalition forces were able to blend kinetic strategic attack with attacks in cyberspace. A primary target was the headquarters of the Republican Guard. These elite Iraqi units were poised to defend Baghdad and inflict casualties on US ground forces. “We started striking Republican Guards headquarters [at] minute one, and we never let up on them,” Moseley, the Air Force Chief, said afterward.⁴⁰ The strikes, he added, “got us 48 to 72 hours ahead of anything they could do.” As in previous wars, signals intercepts gave coalition commanders strong indications that the Iraqi military had broken down and descended into chaos.

For all that, the net effect of the cyber assault in Iraq was to stoke fresh concerns about potential US vulnerabilities in the cyber domain. Commanders realized that sophisticated, real-time communications and data flow had become far more critical to US forces than it was for any potential foe. US dominance of the battlespace hinged fatally on it. Even as plans were made for improvements, especially for the less well-equipped land forces, the magnitude of the dependence began to sink in.

First, all US operations were dependent upon a hefty communications architecture, with the Air Force most dependent of all. Demand for quicker processing and dissemination of space-based and aerial sensor imagery was big. In spring 2003, forces engaged in OIF consumed bandwidth at a rate 30 times greater than that seen in Desert Storm only 12 years earlier. Total bandwidth in use by CENTAF increased from 113 megabytes per second pre-OIF to 783 megabytes per second after it began. This increase of 596 percent reflected the demand on both space and terrestrial systems. Thousands of hours of full motion video, moving target indicator graphics, and other products essential for dynamic operations took their toll. Cyberspace consumption rates made DOD the world’s biggest customer for satellite bandwidth. Up to 84 percent of requirements came from commercial satellites.⁴¹

36. Bradley Graham, “Bush Orders Guidelines for Cyber-Warfare,” *Washington Post*, Feb. 7, 2003.

37. “Fierce Cyberwar Predicted,” Associated Press, March 3, 2003.

38. Graham.

39. “Operation Iraqi Freedom: By the Numbers,” US Central Command Air Forces, April 30, 2003.

40. Author interview, Lt. Gen. T. Michael Moseley, commander, USCENTAF, July 24, 2003.

41. Clay Wilson, “Network Centric Warfare: Background and Oversight Issues for Congress,” Congressional Research Service, Updated March 15, 2007.



could not be left to chance. Attacks on the Iraqi systems and the heavy reliance and safeguarding of US systems put cyberspace in a new light.

It was not that American forces would be unable to fight without cyberspace control. Undoubtedly, they'd do it with radio voice communications and aerial reconnaissance and visual targeting, if need be, but the dramatically large American edge in conventional warfare had now grown cyber-dependent. The National Military Strategy of 2004 spoke of adversaries that might "threaten the US throughout a complex battlespace," defined as "airspace, space, and cyberspace." To all intents and purposes, cyberspace was now a place all to itself.

HIGHER PRIORITY

Following the major combat phase of OIF, cyberspace became a preoccupation of top Air Force leaders. In time it also became an official mission priority. Moseley and Wynne together, in December 2005, signed out a new mission statement for the Air Force. It read, in pertinent part: "The mission of the United States Air Force is to deliver sovereign

Army Gen. Hugh Shelton, then JCS Chairman, presided over development of "Joint Vision 2020," with much greater emphasis on information operations.

Second, the exploitation of cyberspace blossomed as a tactical option for speeding up command and control. One example: Secure Internet relay chat rooms. From the air operations center to ground forces units in the field, multiple-user secure Internet chat was often a primary means of conducting operations. The chat programs used were commercial, but the networks on which they traveled were secure. Cyberchat was limited only by access.

In the opening campaign of OIF, the air component was extremely dependent on information flows through cyberspace. In fact, without it, conducting joint air and other operations at desired levels of intensity would not have been possible. CENTAF reported that "during the three weeks of the war, no [air] base experienced any significant outage of communications."⁴² That is because commanders concluded that the air component's access to that flow of information

options for the defense of the United States of America and its global interests—to fly and fight in air, space, and cyberspace."

Putting "cyberspace" on a footing equal with both air and space was an eye-catching move. Wynne and Moseley described all three as "commons"—that is, distinct, global domains that should be kept free of the control of adversaries or anyone else who would inhibit the world's unfettered access. Just as the Air Force long had made free use of air and, more recently, space, it now was serving notice that it intended to operate freely in cyberspace. It was real and important as any physical realm. The unmistakable corollary to this was that USAF would make a point of assuring US freedom of operation in all three domains.

"If we can decisively and consistently control these commons, then we will deter countless conflicts," said the two service officials in a Dec. 7, 2005 joint letter to airmen on the new mission statement. They continued, "If our enemies

42. "Operation Iraqi Freedom: By the Numbers," US Central Command Air Forces, April 30, 2003.

underestimate our resolve, then we will fly, fight, and destroy them.”

As Wynne explained it, however, moving cyberspace up to equal priority simply recognized the realities of the Air Force’s existing situation. “We have quite a few of our airmen dedicated to cyberspace,” he said.⁴³ These airmen, Wynne added, are focused on “security awareness, making sure the networks can’t be penetrated, as well as figuring out countermeasures.” The Secretary went on to say, “The Air Force is a natural leader in the cyber world and we thought it would be best to recognize that talent.” And for all of the attention to cyberspace, USAF did not at first move fast to explain and explore the implications—at least not in public view. Its 2006 posture statement dwelled on traditional concerns such as the threat of advanced surface-to-air missiles to its fighters or the crisis in aircraft recapitalization. It contained scant mention of cyberspace.

Formal emphasis on cyberspace, however, did come from the Office of the Secretary of Defense. In February 2006, it released the 2005 Quadrennial Defense Review Report. This QDR study complained about the ability of terrorists to “exploit the Internet as a cyber-sanctuary”⁴⁴ and warned that DOD would maintain a deterrent posture to show that “any attack on US territory, people critical infrastructure (including through cyberspace) or forces would result in an overwhelming response.”⁴⁵ The Pentagon’s concern stemmed, at least in part, from evidence that China was “likely to continue making large investments in high-end, asymmetric military capabilities, emphasizing electronic and cyber-warfare.”⁴⁶ Elsewhere, the QDR adduced a conservative

An F-16 of the 510th Fighter Squadron, Aviano AB, Italy, in 1999 flies over Serbia. The Air War Over Serbia featured some cyber war operations.

view of ways to “advance net-centricity.” It affirmed the importance of completing the Global Information Grid (GIG) and developing a stronger and more consistent data strategy across the department. In fact, the QDR explicitly favored shifting from “military-service-focused efforts toward

a more defense-wide enterprise.”⁴⁷ Like the Air Force up to that point, DOD did not go too deeply into the combat implications of cyberspace.

However, the Air Force was pushing forward. USAF in January 2006 created a Cyberspace Task Force under the direction of Dr. Lani Kass of National Defense University. Senior officials also conferred with Cartwright because the STRATCOM commander held national authority for cyberspace operations. Cyberspace was a major topic at the Air Force’s July 2006 Corona conference on warfighting priorities. Two significant actions followed. Air Education and Training Command began to explore training and career field progression of cyber operations in the Air Force. Second, and even more dramatic, Elder, the commander of 8th Air Force, was tasked to build a roadmap for creating a new Air Force major command.

These USAF initiatives were well underway by November 2006, a month in which Wynne delivered a major address on cyberspace as a warfighting domain—the first such public statement ever made by an Air Force official.

Wynne’s premier point was this: “[The] ability to fight in ground, sea, air, and space depends on communications that could be attacked through cyberspace.”⁴⁸ Wynne was saying, in short, that the information dependence of Air Force systems, by itself, was enough to redefine a domain. Moreover, he



USAF photo

43. “Air Force Releases New Mission Statement,” MSgt. Mitch Gettle, Air Force Print News, Dec. 8, 2005.

44. Report of the Quadrennial Defense Review, Feb. 6, 2006, p. 21.

45. QDR, p. 25.

46. QDR, p. 29.

47. QDR, p. 58-59.

48. Secretary of the Air Force Michael W. Wynne, “Cyberspace as a Domain in which the Air Force Flies and Fights,” Address to the C4ISR Integration Conference, Nov. 2, 2006.

went on, terrorists, criminal financiers, drug dealers, foreign hackers, and foreign operatives to use cyberspace as part of the sequence of their actions. As Wynne noted, any terrorist with a cell phone or hacker with a laptop computer today would find that their “use of cyberspace is uncontested.”

Wynne declared to his audience, “My duty as the Secretary of the Air Force is to put the nation’s most technologically capable force on a path to do our share of the task of presenting to our combatant commanders, and so to the President and the nation, the trained and ready forces they may need to ensure the same security and freedom of cyberspace that Americans and indeed many in the world already enjoy in the oceans, in the air, and also in space.” Wynne emphasized that the Air Force was not out to gain complete control. Rather, he wanted to establish the idea that “freedom of cyberspace may in time be the same kind of principle as freedom of the seas and freedom of the skies.”

DEFINING THE DOMAIN

The Air Force, however, was coming up against some basic questions. What is cyberspace? Where is cyberspace? Where does it begin, and where does it end? Other domains—air, space, sea, and land—have clear physical and geographic limits. The domains of air, land, and sea are self-explanatory in nature. Space, though less clearly defined, nevertheless is delimited by a widely accepted lower altitude level separating it from air.

Not everyone greeted the Air Force statement with applause. “The doctrinal piece of domain is still an area for negotiation,” cautioned Cartwright.⁴⁹ “Rushing to the end game...you want to be careful about that,” he added.

Understanding cyberspace as a domain was trickier, even after most acknowledged its battlefield role. The Joint Staff’s Joint Net-Centric Campaign Plan of October 2006 issued a definition of cyberspace as “a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”⁵⁰ By selecting the electromagnetic spectrum as the physical location of cyberspace, a conceptual problem was solved: The realm of cyberspace would not be limited merely to “the Internet” or defined by some particular number of routers or computers or users.

The Air Force also embraced use of the electromagnetic

spectrum as a way to define cyberspace dominance. “The domain is defined by the electromagnetic spectrum,” said Kass, who was given the title of Special Assistant to the Chief of Staff for Cyberspace. “It’s a domain just like air, space, land and sea. It is a domain in and through which we deliver effects—fly and fight, attack and defend—and conduct operations to obtain our national interests.”⁵¹

However, it was not enough just to tag cyberspace as a reflection of the electromagnetic spectrum. That “place” contains waveforms of energy ranging from gamma rays and x-rays at one end through visible light in the middle to microwaves and radio waves at the other end. Locating cyberspace in the EM spectrum, in other words, was a necessary but not sufficient definitional step. Many things happen within that spectrum, but they are not all equally relevant to cyberspace. The DOD definition—with its emphasis on exchange, storage, and modification of data—took the conceptual task much closer to completion. It was saying that what mattered most was not the electromagnetic spectrum itself, but how it was actually put to use.

Here, the history of communications offered a useful way to measure and assess, and thus define. For the most part, so-called revolutions in communications have been measured two ways. The first was change in the relative speed of information exchange—from word of mouth to the pony express, for example, or from radio to cell phones. The second standard was the degree to which a particular communication technique comes to permeate the lives of its users. For example, television could be said to have reached a sort of tipping point in the 1960s, said one of the early elaborators of cyberspace. TV at that stage had become “a medium not unlike the air itself—surrounding, permeating, cycling, invisible, without memory or the demand for it.”⁵²

Major communications revolutions, of course, moved beyond relay systems and line of sight communication. Man progressed from the telegraph in the 1830s to the telephone in 1877 to wireless transmissions in the 1890s and television in the 1940s, but went on to bigger and better things.

Communications have played major roles for a long time in military operations, logistics and intelligence. Sneaking into a foe’s communications began early on. Wiretapping of telephones dates to the 1890s. Surreptitious intercepts of telegraph messages occurred even earlier, in the Civil War. World War I gave rise to the first signals intelligence

49. Author interview, Gen. James E. Cartwright, vice chairman, Joint Chiefs of Staff, Sept. 14, 2007.

50. “Joint Net-Centric Operations Campaign Plan,” Joint Chiefs of Staff, October 2006.

51. John C.K. Daily, “US Air Force Prepares for Cyber War,” UPI, Oct. 9, 2006.

52. Michael Benedikt, Ed., *Cyberspace: First Steps*, (Cambridge, MA: The MIT Press, 1991), p. 10.

exploitation. Cyphers and cryptology took off at the same time. In the years before World War II, major military powers built up sophisticated radio-based intelligence functions and code-breakers.

Yet, while electronic transmissions were subject to intercept and decryption, stored data for a long time remained virtually untouchable by electronic snoops. Obtaining foreign government code books required physical espionage and break-ins—all of which the US military conducted with great skill, and in great secrecy.⁵³ It was always at the moment of the “exchange” of data that the spy did his work.

Even in the 21st century, the exchange of data—by radio, voice, Internet, or word-of-mouth—would remain a point of vulnerability. However, the rise of cyberspace added two nodes of vulnerability: storage and modification. To be effective, cyber systems must be able to perform all three functions—exchange, storage, and modification of data. Think of modification as the process of editing a text, updating a spreadsheet, adding a piece to a design, or performing calculations. Modification functions are a key source of value. So is the ability to store authentic (that is, modified) data, and to transmit and receive data that is authentic and with its value intact. Anything that affects any of those three processes degrades the system and could be

In 1995, retired Vice Adm. Arthur Cebrowski rated the deterrent power of the new cyberweapons “somewhere between nuclear and conventional weapons.”

called a cyber attack.

Consider the analogy of the home. The first personal computers with their 500-kilobyte active memories opened the door for storage of data and a new functionality, from writing term papers to playing computer games. In the 1980s, the availability of limited subscriber networks connected over telephone modems created the first multi-user cyberspace domains. Many were built around community message board formats. Even in the 1990s, the typical American online account did not exactly whip up a full, interdependent cyberspace environment from day one. Cyberspace remained an area of limited transaction.

In the 1990s, massive expansions of computer memory and growth of the Internet transformed cyberspace into

something more than a literary concept. After 2000, greatly expanding Internet access allowed users to transfer more and more valuable functions to cyberspace. Then came cheap desktop computers, Blackberries, iPods, online banking, e-mail, computer faxes, chat rooms, Face Book, and so on. For the individual, the linking of these devices and the wealth of information that they contained created a new domain of value. Cyberspace, then, required two things: networks, and the functional devices attached to them.

At this point, something did *not* happen, and the fact that it did not was extremely important. Cyberspace did not become a closed, exclusive, or all-encompassing realm. Even as cyberspace became functional enough and valuable enough to be a legitimate domain of human activity, it maintained strong connections to and exerted a great



DOD photo

influence on the physical world.

One prime example was the experience of early cyber retailers. Many big successes were “bricks and mortar”

53. Edwin Layton, *And I Was There*, (New York: William Morrow, 1985), p. 79. Layton describes a 1935 break-in by a Navy chief and lieutenant at the home of the Japanese naval attaché. Unable to find a coding machine, the cryptanalysts eventually built their own, the redoubtable “Purple” machine which cracked Japan’s diplomatic code.

storefront companies that augmented their shopping-mall stores with an online presence with the same branding, marketing, and customers. Life could go on without cyberspace, if necessary, because the bulk of the transactions—personal, social, and economic—were still taking place outside of cyberspace, in the “real” world.

With the stupendous rise of the Internet in recent years, a much larger percentage of transactions take place in cyberspace, not in the “real” world. How important is the cyber domain? That depends on the extent to which cyber transactions connect with and influence physical ones, and how important those transactions are. Hitting cyberspace with a worm that impairs the Internet or a virus that crashes your computer wipes out those transactions, at least for a time. This type of disruption may be inconvenient merely, or it may be deadly.

An air operations center in Southwest Asia. USAF has declared “the air operations center is a weapon system” used to exchange, integrate, and act on information quickly.

PAST THE TIPPING POINT

One way to assess the role and impact of cyberspace is through a set of criteria demarcating a usable domain. A team of researchers in 1993 suggested a set of criteria that stated as a proposition: “A typical case of a distributed cyberspace will involve many objects acting in concert to support a rich set of tasks.”⁵⁴ Criteria included richness, connectivity, persistence, and direct interaction. Each of these helped define what creates a valuable cyberspace domain. Richness referred to the value and significance of the user’s experience. Connectivity measured an object’s power to communicate with other objects. Persistence meant storage and use of information and the continuity of such information. Direct interaction was defined as a situation in which “gains outweigh the costs.”

That framework meshed well with the military cyberspace, too. E-mail, chat, electronic invoicing and a multitude of other web-based functions are greatly preferred over old media such as the telegram, interoffice memo, or even the telephone. The point is that cyberspace is not a singular community closed off from any other domain. Nor is it the only domain in which humans can function. Naturally, one person’s dependence upon cyberspace will differ from

another’s, whether the subject is e-mail, online banking, ATM visits, travel reservations, or editing. Certain functions can create massive value for one person and almost none for another. The same is true in the world of armed operations. What makes a domain is, to a large extent, the aggregate value of cyberspace activities.

By 2005, the Air Force had come to believe that, when it came to cyberspace, it had already passed the tipping point. USAF officials concluded that cyberspace was essential in its own right and in connection with other activities. For airmen, then, cyberspace can be thought of as a realm of networks with a degree of richness, connectivity, persistence, and direct action sufficient to constitute a distinct domain.

For airmen, defending the ability to use established



USAF photo/Sr.A. Brian Ferguson

cyberspace systems that enhance the application of air and space power amounts to Job One in cyberspace. The first role of that domain is to make possible what the Air Force calls “cross-domain operations.” Simply put, the execution of critical tasks in air and space now depends on cyberspace functions. The sure flow of information to command and control networks or to airborne battle networks became integral to the success of Air Force operations a long time ago. Elder said he worries about “an adversary that can go in and could take away our domination of cyberspace.”⁵⁵ For the Air Force, he warned, “it means taking away the speed, range, and flexibility that we provide to the Joint Force commander.”

The Air Force, thus, has much to lose if a foe ever could

54. Michael Benedikt, Ed., *Cyberspace: First Steps*, (Cambridge, MA: The MIT Press, 1991), p. 418-21.

55. Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, Defense Writers Group roundtable, June 13, 2007.

manage to dominate key parts of the domain. According to Elder, the Air Force “must make certain that we can control the domain” as USAF controls air and space. “For our own use, we absolutely have to have domain control. If we can’t communicate with the aircraft, if we can’t communicate with the spacecraft, we can’t do our mission.” To that end, the Air Force stood up Air Force Network Operations Command in August 2006. Network operations ensured that the Air Force cyberspace networks were secure and functional. Think of it as the Air Force’s home base for cyberspace warriors.

Before the change last year, network operations were split across different units. “Previously, we had commands focused on air and space forces, but no command focused on operations in cyberspace—that’s what we’re going to provide here,” Elder explained.⁵⁶ The reorganization streamlined Air Force capabilities for network defense, for example. “AFNETOPS command will improve coherency, responsiveness, and agility of network defense against our increasingly numerous and sophisticated adversaries,” said Col. David J. Pistilli, who was then the detachment commander.⁵⁷

The 2006 move also spurred the process of presenting integrated capabilities for the Joint Force. “The biggest benefit of standing up a command structure for Air Force network operations is that it unifies command of the Air Force computer network under one person, who serves as the Air Force component commander and presents network operations forces to USSTRATCOM’s Joint Task Force-Global Network Operations,” Elder said.⁵⁸ The move also consolidated Air Force Network Operations Security Centers, forming major centers at Langley AFB, Va., and Peterson AFB, Colo. Both fell under the renamed 67th Network Operations Wing, at Lackland AFB, Tex. At the core of all of this is a virtual organization, Air Force Network Operations Center or AFNOC. It has three divisions—at Barksdale AFB, La., Lackland AFB, Tex.; and Maxwell AFB-Gunter Annex, Ala.

These organizational shifts have laid down the groundwork for the Air Force to establish a major command devoted to service cyber operations. As with any US armed service activity, the work is limited to organizing, training, and equipping forces to be used by combatant commanders. At present, no one is sure which command or commands will

acquire operational suzerainty in cyberspace. Some believe that, over time, STRATCOM will focus on cyber operations as its primary mission. If that proves to be the case, Air Force Cyber Command would probably become its main component.

THIN LINE TO THE SATELLITE

Protecting cyber capabilities is not only a task to be carried out in the virtual world. To exploit the electromagnetic spectrum, airmen must harness it in the physical world of atoms and waves—the “real” world. Securing the world’s fiber optic strands, satellite links, and coaxial cable, all manifestations of the physical world, will prove to be as important to cyberspace dominance as clever keystroking.

For airmen, a major challenge is to deploy and sustain networks in austere and dangerous expeditionary operations. The massive resources of fiber and coaxial cable supporting the Internet in the United States did not at first exist in the deserts of the Middle East. Secure networks had to be constituted *de novo* for in-theater use in order to provide warfighters the information advantages and reach back they’ve come to expect. Satellites became critical to rapid data exchange. As Elder puts it, “We are connected by thin line to the satellite.”⁵⁹

The act of creating cyberspace for expeditionary use depended on extending several information nets into the theater. Some of these, such as airborne networks, could be set up with airborne platforms. Elder noted, “It’s like deploying AWACS; we interleave satellite, ground, and air networks.” Deployed USAF forces use cyberspace for their own functions and provide these capabilities to the Joint Force. Maintaining smoothly functioning networks is essential. “We always think about our expeditionary capability in terms of moving people and equipment any place in the world,” said Elder.⁶⁰ “You have to realize we can go to any part of the world and we can start doing operations immediately because we can stand up the communications, the command and control systems, situation awareness systems, that we need to be able to do that.”

Now that ability is subsumed in the cyberspace domain and, to fight well, the Air Force must protect it. “When we talk about cyber defense, we’re not just talking about trying to fit some kind of better virus protection on a computer,”

56. Capt. Carla Pampe, “Air Force Changes Network Operations Structure,” Air Force Print News, Aug. 31, 2006.

57. Pampe.

58. Pampe.

59. Author interview, Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, July 25, 2007.

60. Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, Defense Writers Group roundtable, June 13, 2007.

Aircraft such as this MQ-1 Predator in Iraq feed data into the cyber networks and greatly multiply the power of combat forces.



USAF photo/MSgt. Deb Smith

Elder said. “We’re talking about protecting this ability to do these interdependent joint operations.”

During the 20th century, air superiority grew to be a non-negotiable precondition for victory. However, it was not easy to achieve then, and it is not easy now. Dominating cyberspace will be no different. “Cyber superiority turns out to be hard to achieve,” Elder said.⁶¹ He explained that, though cyberspace is related to a physical domain—in this case, the electromagnetic spectrum—cyberspace doesn’t exist “until it is created.” Therefore, cyberspace superiority involves protecting all the elements of the enterprise: the ability to create networks, the operations of those networks, and the power to attack through those networks. “Fail to any one of them,” said Elder, “and cyber is out.”

The first key to cyberspace superiority is survivability. Here, the Air Force’s cyberspace domain has weak spots. First is the physical infrastructure that harnesses the electromagnetic spectrum. Expeditionary combat operations depend on satellites. The Air Force style of expeditionary operations “assumes satellite-based information service is available anywhere on the planet,” said Elder. However, adversaries have capabilities that would be useful against satellites—not just kinetic, destructive anti-satellite weapons but also lasers and other capabilities. Failing that, commercial satellite bandwidth can be stolen or rerouted to put the squeeze on information flows. “People are realizing there are fairly inexpensive ways to get at space,” Elder said.

One way to stiffen the service’s cyberspace backbone is by making it redundant. Achieving cyberspace superiority in this way will entail some dirty, hands-on tasks, too. For example, fiber optic cable is still a major means of communication. But there is not enough of it in the right places. Cable was laid all over the Middle East. There is much less of it in places like Africa and certain parts of Asia.

The Air Force will also have to optimize use of satellite bandwidth and other limited resources. Example of recent success: Ground based terminals in Southwest Asia have been feeding some communications out of that area and back to sites in Germany, where the Air Force had access to extensive satellite bandwidth. The Air Force’s job was to analyze and

optimize those access points, said Elder. The good news is that the Air Force has supreme competence in this area.

Smart placement of local networks is another method. Extending the cyberspace structure in theater led to development of RIPRnet (for Radio Over Internet Protocol Routed Network; it is pronounced “ripper net.”) RIPRnet, developed over a two-year period, was built to improve theater communications in Iraq. It allows radio transmissions to move over an Internet router network. This stand-alone network, designed by airmen in CENTAF, routed communications in a way that overcame line-of-site restrictions. Its first application linked the Combined Air Operations Center to aircraft and controllers. Next, RIPRnet technology picked up fixed Army ground radio relay points and extended command and control functions for convoy operations. Ultimately, RIPRnet systems could take the place of aircraft brought in to serve as extended line of site communications relays for the convoys.

SOFTWARE AND HARDWARE

Achieving cyberspace superiority depends, as well, on selection and employment of software and hardware. Software, of course, is a major point of entry for harmful activity—worms, viruses, and phishing programs, the panoply of malware. Elder cited several techniques to improve survivability. One was moving from reliance on individual base servers to reliance on a larger, consolidated set. Another is using techniques—many similar to those in use on the Internet and by corporations—to enhance safeguards. For example, a key problem is detecting intrusion into an operating system. “By moving to a standard client configuration,” said Elder, “it is possible to check to see if each system matches and to monitor modifications of the

61. Author interview, Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, July 25, 2007.

operating system.” Doing so would make it difficult for a malefactor to tamper with the operating system.

USAF has given service-wide priority to educating airmen about attempts to scan the scan and breach unclassified military systems. The Air Force also uses data reproduction to protect the NIPRnet. Users accessing the af.mil domain are redirected to multiple and identical sites where the page content is kept. With many copies of the site and its pages operating at once, network systems can verify authenticity by comparing all pages to each other. This will more quickly reveal intrusions and tampering.

Vulnerability can be attributed to hardware as well as software. Elder said disruption can stem from “anything you do that introduces ions” to a system. (An ion is an atomic particle carrying an electric charge.) Ever wonder why secure facilities bar compact discs and flash drives? Cheap hardware picked up at a tradeshow or some other seemingly innocuous place can and often do contain hidden programs that will occupy a computer and let adversaries come in behind the firewalls. No wonder that guard at the will not admit your device.

There are far more sophisticated attack methods. On a computer chip, performance depends on the speed with which ions zip around the circuits. Bombarding the chip with a heavy dose of directed energy is one way to disrupt those ions and unravel the cyberspace systems they create. Elder said it takes “serious power levels” to push a system off line, but less power just to “introduce an error message” in that system, which may be enough to achieve the adversary’s goal.

As both the Air Force and Defense Department have acknowledged, the US military already possesses some formidable offensive cyber weapons of its own. It’s safe to assume that there is nothing done by today’s hackers and crackers that cannot be done better and faster by US military cyber-warriors. Elder doesn’t even try to disguise that fact. In fact, he outlines three major worlds of cyber offense. They are:

- **Physical:** The Air Force could drop smart bombs or non-lethal carbon filament weapons to eliminate power or cooling to an adversary computer system. Result: a shutdown, either for a short time or forever.

- **Virtual:** Here, the target could be routers—in ways not unlike some of the bigger public Internet attacks. The attacks on Estonia targeted primarily the virtual network components. Perhaps using methods similar to well-publicized attacks, airman in cyberspace may be able to inject code that interrupts an enemy network, imperils the operating system, or slows it down.

- **Cognitive:** By interfering with and changing data, “users

can’t trust what’s happening,” said Elder. Then, even if a set of information is valid, an adversary will not be able to rely on it and instead choose to operate in the dark.

Any or all of these approaches could be used to mount a devastating cyberattack. It’s important to note that any major US cyber offensive would not target the global Internet *per se*. A much more lucrative—and difficult—target would be the secure, limited-access computer networks of adversaries. A future attack option might be using cyberspace tools to degrade control systems in the electric grid without conducting any physical attack at all. The laws of war that justify precision bombing of targets in the power grid would seem to apply equally to malware attacks on that grid.

Viewed in a traditional way, cyberspace superiority is nothing more than a complement to air and space supremacy. Cyber attacks fit well into the airpower concept of strategic attack. For example, targeting of electric power grids took place in Operation Desert Storm in 1991. Aircraft bombed generators with the goal of diminishing power supplies for military command and control and other operations. Here the relationship between air, space, and cyberspace is critical. Objectives set for other phases of the campaign may shape key requirements for cyberspace attack options. For example, commanders may task cyberwarriors to disrupt or disable an integrated air defense network when fighter aircraft are attacking. However, there will also be times when cyberspace options are not enough. Commanders may have to decide: do they want a surface-to-air missile cut off from its network, or do they want it destroyed so that it won’t be running again in 24 hours?

Integration is already the watchword at 8th Air Force. “At Barksdale, we rarely talk about just cyber,” said Elder. “It’s all part of an integrated effort.” Elder expected cyber expertise to be integrated through the air operations center across strategy, plans, and combat operations. He rejected the idea of a separate force, as was the case with space and even mobility forces, in the early days. Instead, Elder said, he wanted to see a fully integrated set-up, ideally with cyberspace providing “forces via [the commander of Air Force forces] for operations in theater.”

PEER COMPETITORS?

The possible terrorist use of the Internet for nefarious purposes gets much of the publicity, but the Air Force must take a broader view of the challenges in cyberspace. “We have peer competitors right now in terms of dealing with computer network attacks through computer network exploitation,” said Elder.⁶² And compared to these peer competitors, the terrorist Internet threats appear to be relatively tame.

62. Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, Defense Writers Group roundtable, June 13, 2007.

Who are the adversaries? “Any country that you can think of as a potential adversary is scanning our networks, so pick an adversary,” said Elder. He quipped, “Actually, everyone but North Korea. We’ve concluded that there must be only one laptop in all the country, and that guy’s not allowed to scan.”

A Strategic Command official outlined a kind of hierarchy of threats. Tier I consisted of “kiddy hackers”—talented but mostly nonpolitical individuals cracking the net. Tier II comprised operators with more advanced skills, but with capabilities that are much less imposing than those of a nation state. Tier III were the peer competitors with “NSA-like capabilities plus nation state resources” behind them. The United States, Britain, Russia, China, and a smattering of European countries all fit into this Tier III compartment.

STRATCOM is taking a hard line on countering anyone who would put cyberspace at risk. According to command officials, the best strategy of deterrence is to engage in offensive cyberspace operations. “We are engaging these cyberspace attacks offshore, as they seek to probe military, civil, and commercial systems,” said Cartwright in March 2007 testimony. He emphasized that this offshore work would be “consistent with principles of self defense” and aim mainly at defending the Defense Department’s portion of the Global Information Grid.

Traditional military options such as deterrence may or may not work in this new realm. Cartwright, who was confirmed as vice chairman of the Joint Chiefs of Staff in August 2007, drew a historical parallel with nuclear deterrence. During the Cold War, decision makers could count on knowing “without a doubt” where an inbound nuclear weapon was coming from. “We had a way of talking to each other nation to nation both in words and actions that kept us from going over the brink,” said Cartwright.⁶³ “This cyber activity right now does not come with a home address.”

Ideally, offensive operations would give STRATCOM the ability—if ordered—to quickly shut down adversarial activity. Such activity might be traced back to intruders scanning networked systems, but don’t expect to see STRATCOM taking down a bad-guy banking system just yet. For the time being, the offensive tools are still primarily in support of kinetic effects in air and space, according to a Strategic Command official.

Even so, it is true that STRATCOM is committed to moving beyond defensive network operations and taking preparing to go on the offensive, when necessary. “To date, our time and resources have focused more on network defense, to include firewalls, anti-virus protection, and vulnerability scanning,” Cartwright said. “While generally effective against unsophisticated hackers, these measures are marginally effective against sophisticated adversaries.” Cartwright went on to say that a defensive “Maginot Line” posture was too risky for the United States to embrace. The nation was “better served by capabilities enabling us to take the fight to our adversaries.”

“I believe that we’re going to be able to ratchet up our capability [and use] the intellect and the technological might of the nation.” Elder said.⁶⁴ “We’re going to go way ahead. You have to realize that we can go to any part of the world and we can start doing operations immediately because we can stand up the communications, the command and control systems, situation awareness systems.”

The Air Force’s next challenge may come a role in the defense of American cyberspace. Compare cyberspace with airspace. US Northern Command has responsibility for preventing intrusion into American airspace. Considerable effort went into improving defense of the skies after 9/11. Recently, there has been new concern with free and open access to space, too. Unlike air and space, however, US cyberspace is the scene of massive intrusions on a daily basis. When Cartwright warned that America was under constant attack, the secure military network systems were not his only concern. He said the attacks also are targeting commercial and federal civil systems.

Will the Air Force eventually be called on to protect the Internet? “Our nation’s neural network depends on cyberspace,” Wynne wrote in the spring 2007 *Air & Space Power Journal*.⁶⁵ “Free and open use of cyberspace has become an essential tool of the global economy,” said Cartwright.⁶⁶ Indeed, concerns about the safety of the Internet emerged more than a decade ago. President Bill Clinton was the first to try to formulate a national strategy. After several rewrites, it was delivered to faint applause. Then in 2003, the National Strategy to Secure Cyberspace refocused attention on countering the vulnerabilities.

These concerns tend to fall into two camps. First is the difficulty of protecting everyday access to cyberspace and

63. Author interview, Gen. James E. Cartwright, vice chairman, Joint Chiefs of Staff, Sept. 14, 2007.

64. Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, Defense Writers Group roundtable, June 13, 2007.

65. Michael W. Wynne, Secretary of the Air Force, “Flying and Fighting in Cyberspace,” *Air & Space Power Journal*, Spring 2007.

66. Gen. James E. Cartwright, commander, US Strategic Command, testimony, House Armed Services Committee, March 8, 2007.

of insulating the US economy and way of life from cyber disruptions. Second is the danger of cyber attacks on the infrastructure as an additional weapon of war. Currently, DOD sponsors the Computer Emergency Response Team Coordination Center (CERT/CC), while the Department of Homeland Security, in partnership with private industry, operates a parallel organization called US-CERT, which has international counterparts. The Pentagon actually started the CERT emergency response teams to help track malware incursions and to guide recoveries.

However, some want the federal government—and perhaps the Pentagon—to do more. Cyber incursions have become an increasing cost burden for major business. A Strategic Command official estimated that cyber security costs, which once hovered at around two or three percent of gross corporate revenue, have now reached 10 percent in some cases. The costs come from security measures, losses due to theft and piracy of commercial properties. A bank whose customers fall prey to a phishing scam may opt to

USAF photo/SSgt. Cherie Thurlby



Numerous fighters (such as these three F-16s) and bombers were retargeted while airborne in the wars in Afghanistan and Iraq. It could not have been done without mastery of the cyberspace domain.

make good the money they lost, for example.

“You are at a point in my estimation where American business can no longer accept being attacked, discovering what the virus was, waiting a couple of weeks for a company to make a patch, mailing it to you, because the money you lost in that amount of time has exceeded what you can pass on to the consumer,” said Cartwright.⁶⁷

Because of rising costs and the impact on business, the cyberspace debate at the national level is different from the one taking place at Barksdale. Senior executives have petitioned the President to do more. As a result, the Bush administration tasked STRATCOM to think through a new strategy. “Debate is going on with the President as we speak,” said a command official.

TWO PRONGED ATTACK?

The second cyberspace worry is that adversaries—terrorist or state-sponsored—will employ cyberspace networks to launch fast, debilitating attacks on United States territory.

This would be a different type of problem altogether. It links attacks on homeland cyberspace systems to other and perhaps physical forms of attack. According to the 2003 National Strategy to Secure Cyberspace, “In wartime or crisis, adversaries may seek to intimidate the Nation’s political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.”⁶⁸

The SIPRnet might be untouched, but a cyber attack that unravels the electronic systems controlling the Hoover Dam water flow could take warfare to an altogether new dimension. It’s hard to gauge the extent to which critical cyberspace systems may be hardened, redundant, and capable of functioning on back-up power and in isolation from wide area networks during a crisis. That’s the big question.

How that debate turns out could have a big impact on Air Force plans. At the moment, USAF’s role is largely confined to assisting first responders (who will probably be operating under guidance of the Department of Homeland Security.)

It’s not the Air Force’s responsibility to fix commercial Internet systems, but the Air Force must support civil authorities if they ask for help. That could mean restoring Web-dependent communications. As yet there’s not a way for the Air Force to reboot the New York Stock Exchange. However, the Air Force is working on methods to quickly set up cyberspace operations in expeditionary locations. In time, tools such as the RIPRnet could in effect provide a reconstitution capability that national authorities could task for use at home, if needed.

The nation is feeling the effect of the long-ago split between military cyberspace and the Internet. As classified cyber networks developed under National Security Agency encryption, the security divide between government and industry grew. By the 1990s, most leading corporations

67. Author interview, Gen. James E. Cartwright, vice chairman, Joint Chiefs of Staff, Sept. 14, 2007.

68. “National Strategy to Secure Cyberspace,” February 2003, p. viii.

were hard at work on closing cyberspace gaps by making their operating systems and Internet-driven products more secure. However, top US cryptographers were by then largely working in isolation. America essentially divided up its encryption resources. Look for more cooperation between government and industry in the future as both tackle the problem of securing cyberspace.

What will it take to make cyberspace secure? Several Department of Defense officials, speaking off the record, have emphasized that cyberspace sits at the top of their list of concerns for the future. They also report that massive efforts are underway to plan and budget for increasing cyberspace capabilities. “I don’t precisely know exactly how much money we are spending right now,” Elder said.⁶⁹ “If you go across the Air Force budget [and] across the Department of Defense budget, and look at all the things that really are cyber-related, it’s a lot of money.”

USSTRATCOM also made efforts to get a handle on cyberspace missions. Part of the problem rests with defining what type of programs, people, and costs fit in a cyber-programming element. Another difficulty is estimating the scope of the mission. “We are well past the \$5 billion per year mark, and I don’t know what the top end is,” commented one STRATCOM official. “The \$5 billion is mostly on defense. We buy huge amounts of software and people to run that, but it’s totally ineffective against Tier III” cyber threats, this official noted.

Cartwright put the services on notice that he, for one, will watch their investment plans closely. Right now, “each of the services has found value” in cyberspace, according to Cartwright.⁷⁰ “They are making their investments and they are letting their money speak about their risk equations. We’ve got enough time to let that play out,” Cartwright said.

The real issue about domain dominance could come up soon – in budget modifications as early as 2009. The Air Force will have to make serious investment and tough trades to impress the joint community with their commitment to cyberspace.

Cartwright said he will watch to see “when it comes to the hard decisions, who will compromise other things” to invest in cyberspace. “That will be a very telling activity,” said the Vice Chairman. “If Service X says I’m giving up this class of toys, for cyber, it will be very telling about their risk equation. If Service Y says this is really important and I’m going to build

a building but I’m not going to compromise my toys for it, that will [also] be very telling.

For now, the Air Force will continue a series of practical steps. Completing the creation and activation of Air Force Cyber Command is one of them. Changing service education and training in order to produce cyberwarriors is another. Elder and others are working on how to lay the foundation for a cyberspace career path in the Air Force on a par with those for other weapons systems and specialties. “We’re looking to set up a professional cadre of cyber operators, enlisted and officer,” Elder said.⁷¹ “We want to bring people into the Air Force from the beginning knowing that they’re going to be a cyber operator and they will have a complete career path in the Air Force doing cyber.”

Still another important step is to train all airman to be able to respond to cyber attacks “without having to wait for the IT guy,” as Elder put it.⁷² “At Balad [the main air base in Iraq], everyone carries side arms,” Elder noted. “In cyber, we can be under attack anywhere.” He plans a cyber safety program, with standards similar to flight safety, for example. Ultimately there will also be benign cyber exercises to test airman’s abilities, and a form of “stan eval” to gauge cyberspace readiness.

EVOLVING DOMAIN

When the Wright brothers went aloft in 1903 at Kitty Hawk, they were entering a domain that was already well known by birds and balloonists. Flight was not new; what was new was human flight. Ten years later the physical and social domain of human flight had developed to the point that it was about to become a dominant part of 20th century warfare.

Today, just a few years have passed since the emergence of the cyberspace domain. The Air Force is set to provide the bulk of the capabilities for cyberspace as a warfighting domain. As with the early days of air and space, there’s much yet to learn.

What’s clear is that, while the cyberspace domain has coalesced, today’s cyberspace is just a sketch of what is yet to come. Cyberspace concepts dating from the 1980s offered a far more detailed vision of cyberspace, where the ultimate end-state is a virtual reality dominant in daily life. Early works on cyberspace came from architects, artists, philosophers, filmmakers, screenwriters, and so forth. Their view of cyberspace was far more complete than the one that

69. Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, Defense Writers Group roundtable, June 13, 2007.

70. Author interview, Gen. James E. Cartwright, vice chairman, Joint Chiefs of Staff, Sept. 14, 2007.

71. Elder, DWG, June 13, 2007.

72. Author interview, Lt. Gen. Robert J. Elder Jr., commander, 8th Air Force, July 25, 2007.

exists today. Progressing through continued technological development will probably change the form of cyberspace many times—with large consequences for the airmen and others who are defending it and fighting in it.

Cyberspace does not negate the physical world. The Air Force has kept that principle in clear view by emphasizing cross-domain linkages between air, space and cyberspace. Warfighters of the future must also remain acutely conscious of how the physical and virtual worlds overlap. “What I’m most concerned about is protecting the decision space and the opportunity space of the 20-somethings” who are the cyberwarriors of the future,” said Cartwright.⁷³

Discussions of cyberspace as a domain work well, for now. Yet it’s already evident that this new domain inevitably touches on concepts of community, politics, legitimacy, and the state going back 400 years. War and its traditions exists in the seams of all these. However, the definitions of war, security, and military strategy are all subject to change. Cyberspace may already be accelerating that change. Expect frequent spirals of change as airmen learn more about how to operate in the cyberspace domain.

It is no wonder, then, that early 21st century America is in debate over the military aspects of cyberspace and the relationships of business, the military, and how each affects the common defense. Most agree that cyberspace should be part of the global commons. Preventing its disruption has become a key 21st century security task.

The Air Force’s willingness to step up early to the cyberspace mission bodes well. The Air Force is uniquely placed to speed the technology and capitalize on the skills of its airmen to master the domain of cyberspace and all its challenges, and use it for American gain.

“We have been a service to take advantage of the intellectual and technical might of our country,” Elder remarked. “In the past we’ve been embarrassed about this, and we shouldn’t be. Technology by itself does not do it. The airmen are what make the differences. Airmen really are different: one, because of their intellectual component and two, because of their skill set, and three, because of the technology we look for them to employ. So cyberspace becomes a natural extension of what we do.”

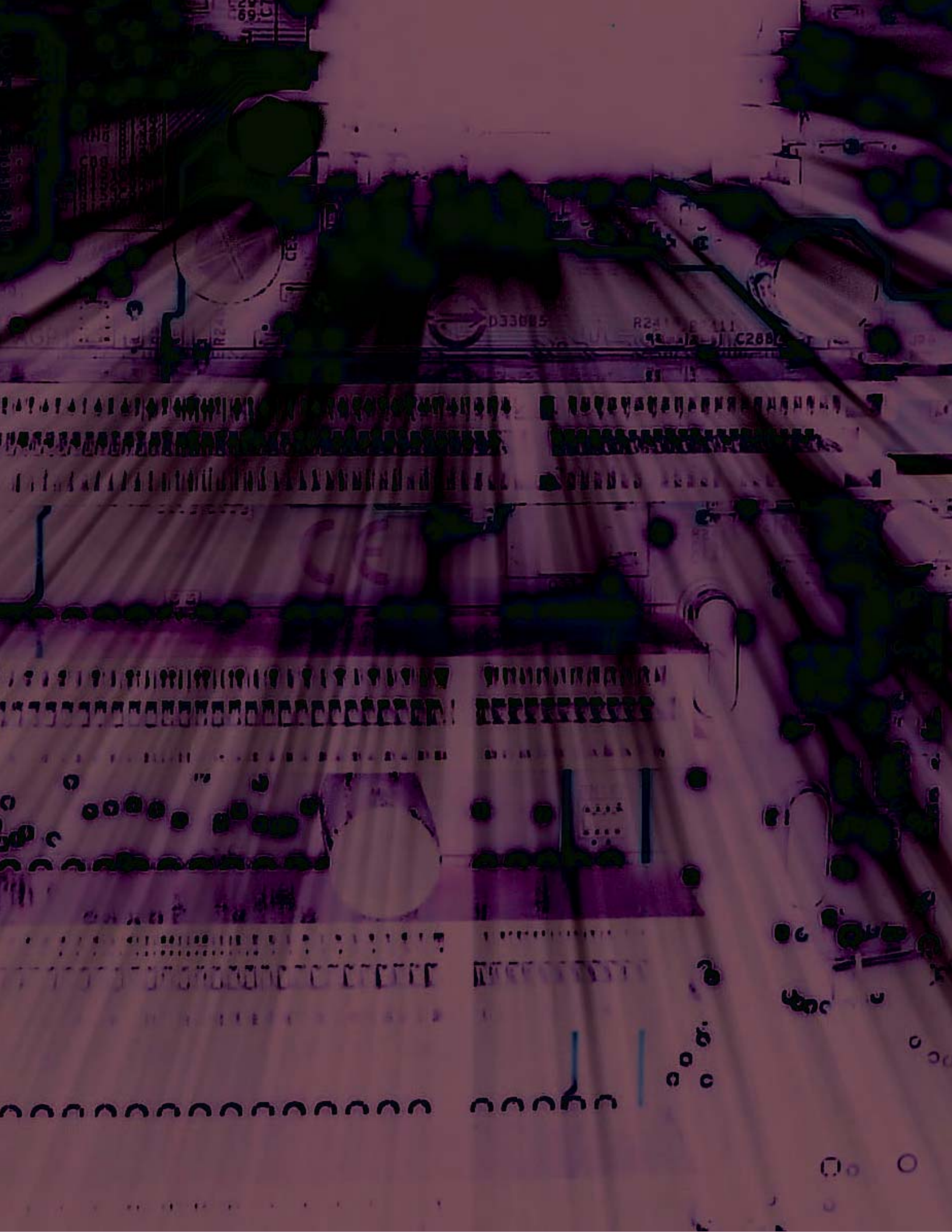
Hap Arnold could not have said it better. ■

73. Author interview, Gen. James E. Cartwright, vice chairman, Joint Chiefs of Staff, Sept. 14, 2007.

NOTES

NOTES

NOTES



69

CE



D33085

R24

C288

JP

