LESSON 3

The Air Force of the Future

Learn About

- the F-35 Lightning II Joint Strike Fighter, KC-46 Pegasus Aerial Tanker, and B-21 Raider global strike bomber
- current issues in cybertechnology
- current developments in cyberwarfare

The F-35 Lightning II Joint Strike Fighter, KC-46 Pegasus Aerial Tanker, and B-21 Raider Global Strike Bomber

As technology evolves, the Air Force must update its fleet to make sure the United States has the best aircraft available. Given the time it takes to design, test, and build today's sophisticated planes, planners are always looking ahead to the next model. The following are some of the aircraft expected become operational soon or that are in the planning stage.

Lockheed Martin F-35A/B/C Lightning II

The F-35 Joint Strike Fighter is an unprecedented—and controversial—attempt to develop one aircraft to replace several different planes. The Air Force F-35A is intended to replace the F-16 and A-10 fighters. The Navy and Marine Corps F-35C variant is intended to replace the aging F-18 fighter.

F-35A Lightning IIs preparing to refuel

Staff Sergeant Madelyn Brown/Courtesy US Air Force

It can operate from any Navy aircraft carrier. The Marine Corps F-35B variant is a vertical takeoff and landing fighter that will replace the AV-8B Harrier. A fifth-generation aircraft, the F-35 aims to provide air superiority, defense, suppression of enemy air defenses, and close air support of ground forces.

In addition, several foreign countries, including Australia, Britain, Denmark, Israel, Italy, the Netherlands, Norway, Singapore, and Turkey are buying the F-35. Three different versions are being produced to meet the requirements of different services and nations.

The F-35 has the most advanced sensors yet on a fighter aircraft. Equipment includes a helmet-mounted display system that shows on the visor all the targeting and intelligence information a pilot needs to complete the mission. Besides Lockheed Martin, Northrup Grumman and British Aerospace are participating in production. Currently, the US military plans to buy up to 2,400 F-35s. Price and budget considerations may affect how many are actually purchased.

An F-35B Lightning II demonstrates vertical takeoff at the Royal International Air Tattoo at Royal Air Force Fairford, Gloucestershire, England.

SpaceKris/Shutterstock

Vocabulary

- cyber
- cybertechnology
- mainframe
- smartphone
- network
- Internet
- hypertext
- protocol
- browser
- social networking
- cloud
- hacking
- encrypting
- firewalls
- social engineering
- phishing
- malware
- whistle blower
- cyberwarfare

A KC-46A (*right*) undergoes testing of its own refueling system. Here it receives fuel from a KC-10 extender, with a KC-135 off in the distance.

Christopher Okula/Courtesy US Air Force

Boeing KC-46 Pegasus

The KC-46A Pegasus aerial refueling aircraft is the first of a three-phase plan to replace the Air Force's aging air refueling fleet. It can carry more fuel, is more efficient, and has more room for cargo and medevac facilities than existing aircraft.

The KC-46A will be able to refuel any fixed-wing aircraft on any mission. A crewmember known as the *boom operator* controls refueling operations. This new tanker utilizes the same air refueling boom as the KC-10. It has center mounted drogue and wing aerial refueling pods. This allows it to refuel multiple types of receiver aircraft from the United States and allied air forces on the same mission. Besides carrying more than 212,000 lbs.—approximately 33,000 gallons—of fuel, it can carry up to 65,000 lbs. of cargo, 15 crew members, and from 58 to 114 passengers, depending on how the aircraft is loaded.

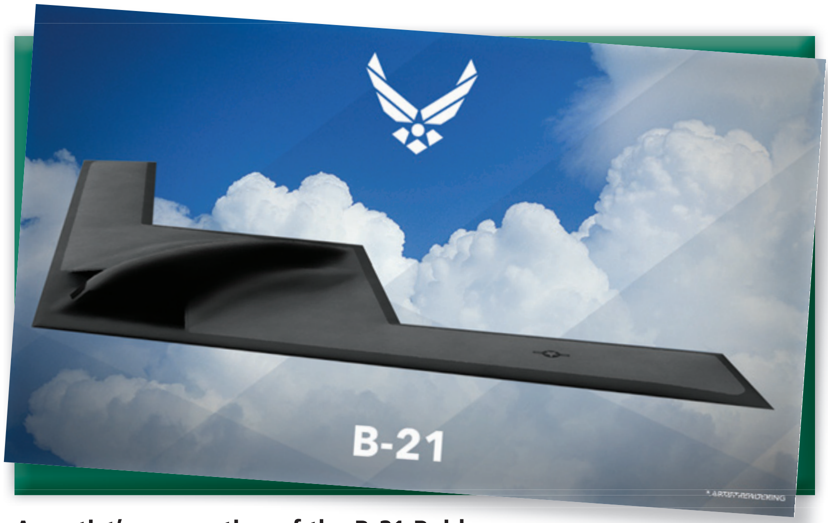
The KC-46A design is based on the Boeing 767 commercial airliner and was approved for production in August 2016. Boeing is scheduled to deliver 18 tankers by early 2018. The company is scheduled to build 179 KC-46 tankers by 2027.

B-21 Raider

In February 2016, Air Force Secretary Deborah James revealed the first drawings of the B-21 Long-Range Strike Bomber (LRBS). The future bomber was named the Raider in a contest among Airmen, honoring the Doolittle Raiders who took off from an aircraft carrier in B-25 bombers to attack Japan during World War II (see Chapter 3, Lesson 2). The B-21 is a key piece in the Air Force's future modernization plans.

The B-21 will give the Air Force the continued ability to launch air strikes anywhere in the world from the continental United States. It shares a resemblance to the B-2 bomber because it builds upon existing and developing technology. Current plans call for the plane to be manned, with an option for an unmanned version.

The first deployment is expected in the mid-2020s. The Air Force hopes eventually to have 100 B-21s.



An artist's conception of the B-21 Raider

Courtesy US Air Force

Current Issues in Cybertechnology

You have grown up in a world full of electronic devices—desktop computers, laptops, tablets, and smartphones. But it wasn't long before you were born that none of these existed.

Cyber is a prefix meaning *computer.* Advances in cybertechnology, or *computer technology,* have affected all the military services, especially the Air Force. Today's civilian and military aviation systems—ground control, air traffic control, and the actual flying of aircraft—wouldn't be possible without modern computers.

But cybertechnology has also introduced new threats and new ways for an enemy to attack the United States—its military, its civilian economy, and the workings of the government itself. To understand what these challenges are and how the United States is meeting them, a brief history is helpful.

An old mainframe computer

Everett Collection/Shutterstock

Evolution of the Modern Computer

The first electronic computers as we know them today were built in Germany, Britain, and the United States in the early 1940s. These were huge machines that used vacuum tubes. It took a whole room to hold less computing power than you can hold in your hand with today's mobile phones.

The first commercially available mainframe computer, the IBM/360, became available only in 1964. A mainframe is *a large, high-performance computer usually connected to several terminals and used by a large organization.* A decade later, the first personal-computer kits became available. In 1977 Apple Corporation unveiled the groundbreaking Apple II desktop computer. IBM followed in 1981 with its release of the personal computer (PC).

In 1984 Apple released the Macintosh desktop. At this time it introduced the "Mac" operating system and the first computer mouse. In 1990, Microsoft released Windows 3.0, which soon overtook the Mac operating system (OS), since the number of PCs sold running Windows far outpaced the number of Macs sold. By early 1990s, some two-thirds of American office workers had a computer on their desk. Portable laptop computers soon followed.

This explosion was made possible by the evolution of computer memory and processing from large vacuum tubes to tiny microchips. As microchips became smaller and more powerful, computers did the same. Data storage moved from very large tape drives as tall as a door to smaller drives, then to $5^{1}/_{4}$-inch floppy disks, then to $3^{1}/_{2}$-inch disks, then to flash or thumb drives.

The introduction of wireless networking, or Wi-Fi, made it possible for computers to communicate with each other without wires and cable. Smaller and smaller chips led to the smartphone and tablet. In 1999 BlackBerry Limited introduced cellphones that could send and receive e-mail. Apple introduced the first smartphone, the iPhone, in 2007. A smartphone is *a cellphone with advanced computing ability.* Apple's iPad tablet followed in 2010.

An early BlackBerry phone

coronado/Shutterstock

Rise of the Internet

From the beginning, researchers wanted computers to be able to share data and computing power. When two computers were in the same building, this could be done by running cables between them. This created a computer network—*one or more computers linked together physically or wirelessly.*

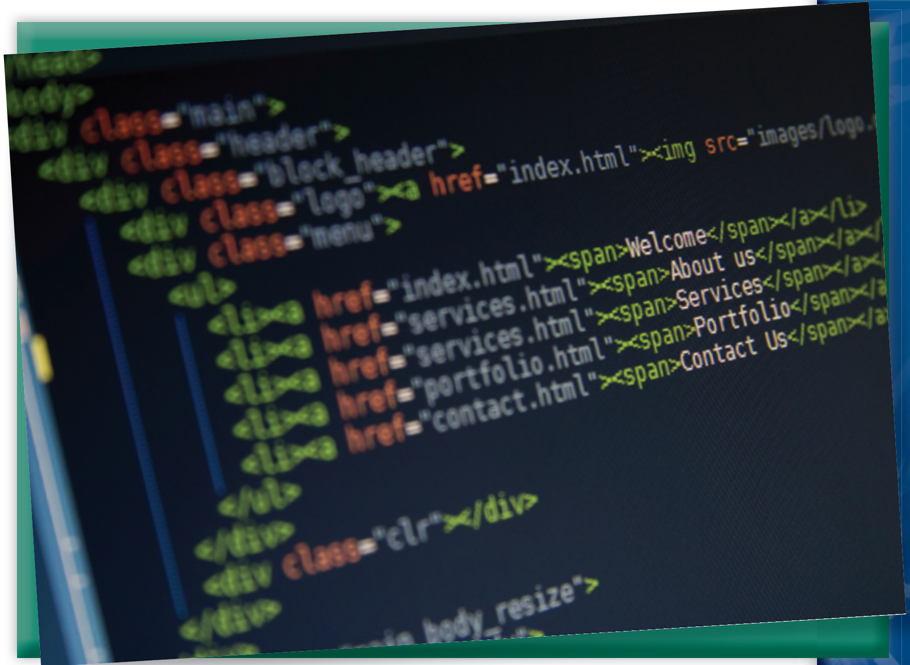
As software developed and became more sophisticated, researchers at the Advanced Research Product Agency (ARPA) in the 1960s and 1970s developed a network of computers linked by telephone lines. (This government organization later became the Defense Advanced Research Product Agency, or DARPA.)

The resulting network was called ARPANET. As computers became smaller and more numerous, and networking technology more powerful, this network grew into the Internet—*a system of networks connecting computers around the world*.

Then in 1989, European researchers Tim Berners-Lee and Robert Cailliau developed hypertext—*digital text that contains electronic links to other texts*. They proposed using hypertext to create a World Wide Web of stored information. In 1990, Berners-Lee designed three important tools that made the World Wide Web (or just "the Web") possible:

- HTTP or Hypertext Transfer Protocol, a protocol, or *an electronic procedure*, used to send files and data over the Internet
- Hypertext Markup Language (HTML)—the code used to create text and documents and set up hyperlinks between them
- the first Web browser—*a program that accesses and displays files on the Internet or World Wide Web*

Web browsers and the Web itself have developed at breathtaking speed since that time. Computer scientists talk about its development to date as three phases—Web 1.0, 2.0, and 3.0.



```
</head>
<body>
<div class="main">
 <div class="header">
  <div class="block_header">
   <div class="logo"><a href="index.html"><img src="images/logo.
   <div class="menu">
    <ul>
     <li><a href="index.html"><span>Welcome</span></a></li>
     <li><a href="services.html"><span>About us</span></a></
     <li><a href="services.html"><span>Services</span></a><
     <li><a href="portfolio.html"><span>Portfolio</span></a
     <li><a href="contact.html"><span>Contact Us</span></a
     <li>
    </ul>
   </div>
   <div class="clr"></div>
  </div>
 </div>
 <div class="main_body_resize">
```

HTML code lies behind each Web page.

Melody Smart/Shutterstock

Web 1.0 is sometimes called the *static Web*. That's because all a Web page did at first was display information. The user did not interact with it. You just read the information, which might not be updated all that often, except for early news sites.

Starting in about 2003, Web 2.0, or the *interactive Web*, appeared. Now the user could interact with the Web page to respond to content, create content, and use online software. This allowed the development of social networking—*interacting with other people through dedicated websites and applications (apps)*. Soon a whole host of social networking apps appeared—first MySpace, then Facebook, Twitter, LinkedIn, Instagram, Google+, and many others. User-generated information sites such as Wikipedia and blogs (from *Web logs*) also date from this time.

With all these people creating all this information, researchers believe the future is Web 3.0. According to Berners-Lee and others, this Web would function as a giant online database that would access, retain, organize, and categorize information. This would allow you to combine multiple searches into one. You could type or say a complex question or sentence, and the browser could pull all the information together for you.

Say you and your friends want to go see a movie and have a pizza afterward. You could type or say "I want to see an action movie and then get a pizza near the theater. What's available?" The browser would search the Web and organize the possible answers for you.

In the meantime, the *Internet of Things* is already becoming reality. Home appliances, automobiles, healthcare equipment and devices, and much more, can now be connected to the Internet. This allows a user to control or monitor them remotely.

Increasingly, people and organizations are storing their data on the cloud—*another name for the Internet*—instead of on their own computers and servers. This allows them to access their documents using any device—a laptop, tablet, or smartphone—anywhere in the world where there is an Internet connection. *Cloud services* mean that people can now also use software located on a remote server rather than download the software to their own computer.

Security and Privacy Issues

You know from your own experience that the combination of computers and the Internet has led to wonderful things. You have more information available to you at a moment's notice than people have ever had before. You can text with your friends while streaming the same TV program. You can play games or work on projects with people all over the world in real time.

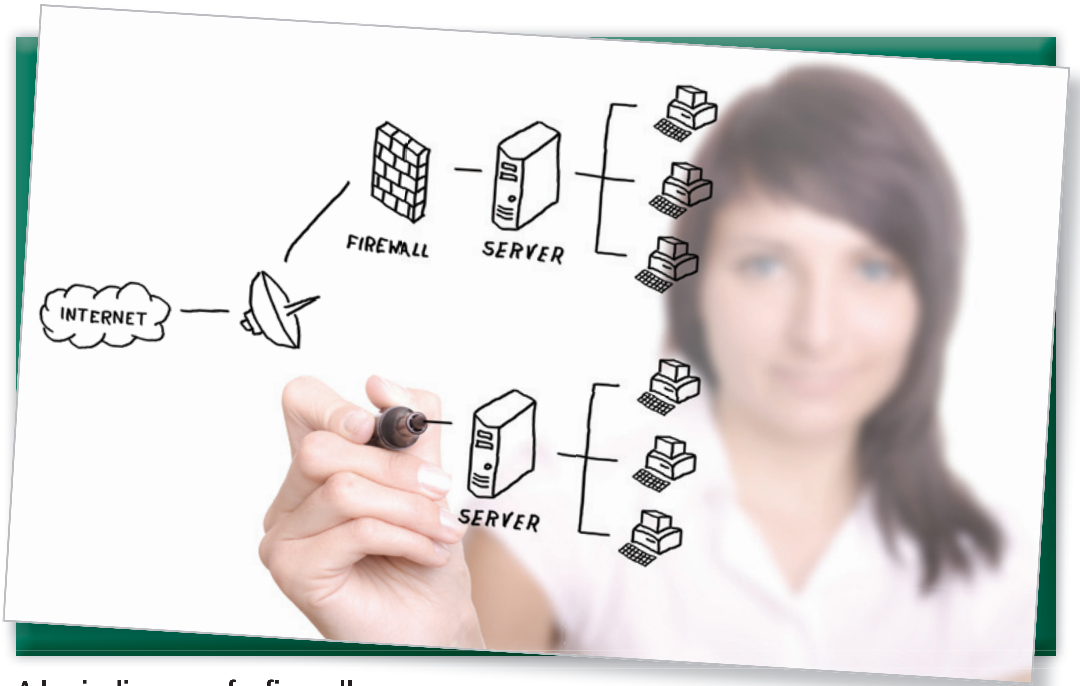
But there is a dark side to this power. While it has opened up enormous possibilities for good things, it has also made it possible for people with harmful intentions to do bad things.

The Internet and computing ability have grown much faster than anyone could plan for. Early developers did not build security into computers, programs and apps, or the Internet. Many commands, e-mails, and messages are sent in the clear—anyone who can intercept them can read them. It did not occur to many people that bad actors would use these new abilities to do destructive things. But as soon as it became possible, it began to happen.

The problem is simple to describe but difficult to deal with. Without proper security, people without authorization can gain access to information stored in computers and on networks. They can steal, change, or destroy information and Web pages. They can gain control of remote devices and make them do their bidding. They can create armies of these machines to launch attacks on other computers and websites to prevent them from operating correctly.

Gaining access to a file, computer, or network that you're not authorized to see is called **hacking**. Some hackers do good work—companies and organizations ask them to test the security of their equipment and systems. These are sometimes called *white hat hackers*—from the days of old movie Westerns, when the good guys wore white hats. Hackers who have harmful or malicious goals are sometimes called *black hat hackers*—because the bad guys in those same movies wore black hats. But many people use the term *hackers* to mean hostile attackers.

Attackers have many ways to gain access to, or penetrate, a computer or network. First, they can get physical access to a machine. This can be prevented by controlling who can get near the equipment. Second, they can try to gain access to the machine over the Internet. If they know or can guess the password, they can log on. An essential defense here is using good passwords, keeping them secure, or avoiding them altogether. Scans of fingerprints, retinas, or faces offer better security. **Encrypting** data, e-mails, and messages—*converting data into secret code*—is another necessary defense. Anti-virus software and **firewalls**, or *programs and devices that monitor and restrict communication between computer systems and outside networks*, are also required.



A basic diagram of a firewall
scyther5/Shutterstock

Another way to penetrate a computer or network over the Internet is to find flaws or "holes" in the software that an attacker can manipulate to gain access. White hat hackers spend a great deal of time looking for these flaws to find them before attackers do. Responsible software companies issue corrections or *patches* to fix the flaws and plug the holes to prevent attacks. Microsoft, Apple, and other tech companies issue regular updates of their software containing these patches. That's why individuals and organizations should update their software regularly, and whenever these corrections are issued.

A third way to gain access is to persuade or fool an authorized user into giving the passwords to an attacker. Attackers also try to trick users into unknowingly loading harmful software onto a device or network that will allow the hackers to gain control of it.

Attackers have many scams to fool users. One is social engineering—*tricking people into giving out sensitive information such as passwords or credit card data*. Another is *shoulder surfing*, which is getting information off users' screens by looking over their shoulders or using a hidden camera to watch while they work. *Dumpster diving* is rummaging through wastebaskets and dumpsters to look for documents or old equipment that many contain sensitive information. *Pretexting* is pretending to be someone else—like a network administrator or a help desk—to trick the user into giving out information.

Another common method of attack is phishing—*tricking people into downloading harmful software or clicking on harmful links in e-mails or on websites*. For example, the attacker will send users an e-mail that claims to be from the users' bank or credit card company. If the users click on the link in the e-mail, they are taken to a website and asked to fill out forms with sensitive information such as their account numbers, dates of birth, mothers' maiden names, and so forth. The attacker can then use this information to gain access to users' genuine accounts and steal their money.

Malware is often introduced into computers on flash drives.

SK Herb/Shutterstock

The following scenario offers another version of this scam: You find a flash drive on the ground in the parking lot. You think one of your co-workers or an important visitor has lost it. You take the drive inside and insert it into your desktop computer to see what's on it and whom it might belong to. But unknown to you, the flash drive loads malware—*harmful software*—onto your computer and the network it's attached to, allowing an attacker to take control.

Methods such as these have allowed attackers to penetrate the networks of banks, large corporations, and government agencies, including the Pentagon. They have stolen people's personal and financial information, sensitive information about company products, classified government security information, and information about weapons systems.

The Inside Job

There's also a fourth way attackers can gain access to information. That's when an authorized user steals the information and sells or gives it to people who shouldn't have it.

There are two well-known cases of this happening to US government agencies. In the first, Army private Bradley Manning in 2010 stole some 750,000 documents stored online. He then gave them to the Wikileaks website. Most of these were classified, and many were sensitive State Department diplomatic messages. Manning, who has since changed her identity to Chelsea, was sentenced to 35 years imprisonment for espionage and stealing government property. President Barak Obama commuted her sentence in 2017 after she had served nearly seven years in prison.

In the second, a government contractor named Edward Snowden in 2013 downloaded sensitive classified information from the National Security Agency and leaked it without authorization to Wikileaks and journalists. Some of the information was widely published. Before the articles were published, Snowden fled to Hong Kong. He later went to Russia, where he has lived ever since. He has defended his actions, saying he was a whistle blower—*someone who uncovers and exposes wrongdoing in an organization*. The US government sees it differently: It has filed criminal charges against him.

Sometimes authorized users steal data.

Andrey Popov/Shutterstock

Who Are the Attackers?

When some people think of hackers, they might think of a young person trying to break into networks as a lark. But most hackers are serious, trained professionals. They may be working on their own. They may be working for organized crime. Or they may be working for a foreign government's intelligence service.

For example, the US government says that in several instances, Iranian government agents have launched attacks against American and European banks. They have overwhelmed the banks' websites with service requests so that the bank sites shut down.

The United States also says attackers working for the Chinese military have attacked the networks of many American companies and stolen their industrial secrets. They have also attacked the US government's own personnel records and stolen information about current and former government employees. In 2014 the United States filed criminal charges against five Chinese military hackers.

The US government has also accused attackers working for Russian intelligence services of attacking US government and commercial networks. During the 2016 US presidential elections, hackers working for Russian intelligence broke into the network of the Democratic National Committee and stole e-mails between officials of the Hillary Clinton campaign and other party leaders. They then gave the stolen e-mails to Wikileaks, who released them to the press. US intelligence officials accused Russia of trying to interfere in the elections by discrediting Mrs. Clinton and other Democratic Party officials.

The increasing number of such attacks in recent years has made it clear that American companies, the government, and the military services face a new type of warfare on a new front: cyberspace.

Hackers in cyberspace attacking computer systems are engaged in a new type of warfare.

Nomad_Soul/Shutterstock

Current Developments in Cyberwarfare

Cyberwarfare is *the use of cyberspace to interfere with an enemy's command and control, disrupt normal economic activity, steal intellectual property or government secrets, and prevent equipment from functioning properly.* As developments over the past few years have shown, this is not fantasy or science fiction: It is happening today. And the Air Force, Army, Navy, and Marine Corps must respond and be ready to fight in this new domain.

As noted earlier, cyberspace attackers can be foreign intelligence agents, terrorists, criminals, or just a lone individual with a grudge against the United States and its allies. Each can cause the same amount of damage. Each is equally a threat.

To counter such threats, the US Defense Department has developed a Cyber Strategy with three primary missions:

- to defend Defense Department networks, systems, and information
- to defend the US homeland and US national interests against cyberattacks of significant consequence
- to provide cyber support to military operational and contingency plans

To implement this strategy, the Secretary of Defense in 2009 directed the commander of the joint US Strategic Command to create a joint US Cyber Command. The new command has its headquarters at Fort Meade, Maryland, which is also the home of the National Security Agency (NSA). The NSA is the nation's signals and electronic intelligence agency. As this is written, the chief of the NSA is also the commander of Cyber Command. However, a debate is taking place in Washington over whether to divide the two.

Cyber Command's mission is both defensive and offensive. Each service has its own command to support the mission: Air Force Cyber Command, Army Cyber Command, Fleet Cyber Command (the Navy), and Marine Forces Cyber Command. Although the Coast Guard is part of the Department of Homeland Security, it also supports the mission through Coast Guard Cyber Command.

The US Cyber Command seal

Adam Hartman/Courtesy US Cyber Command

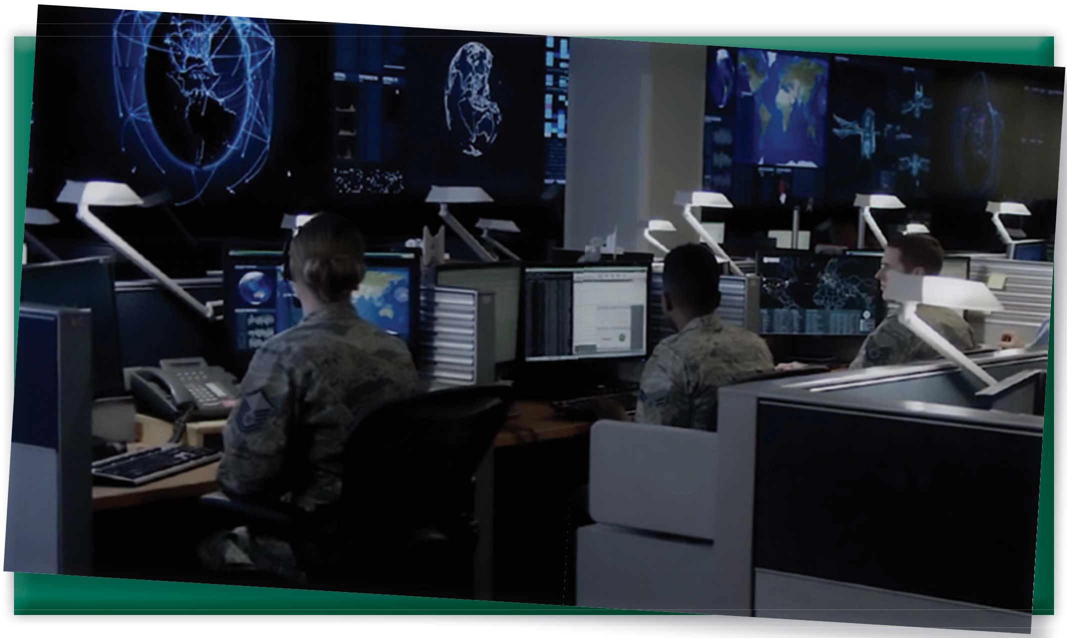
The Defense Department has also organized a Cyber Mission Force of 133 teams with different tasks. Cyber Protection Forces defend against the top threats to Defense Department networks and systems. Combat Mission Forces conduct cyberspace efforts in support of operations. These two types of teams will work with combatant commands in different parts of the world. National Mission Forces defend the United States and its interests against cyberattacks. They will operate directly under US Cyber Command.

Since defending the country in this way involves many departments and agencies of the US government, Cyber Command works closely, not only across the military services, but also with civilian officials as needed.

The Twenty-Fourth Air Force

Air Force Cyber Command is located with the Twenty-Fourth Air Force. Its origins date to 2006, when Secretary of the Air Force Michael Wynne and Air Force Chief of Staff General T. Michael Moseley decided to establish a cyberspace command in the Air Force. In 2008, new leaders Secretary Michael Donley and Chief of Staff General Norton Schwartz, announced the creation of a numbered air force to plan and conduct cyberspace operations. The Twenty-Fourth was placed under Air Force Space Command and headquartered at Lackland AFB, Texas—now part of Joint Base San Antonio.

One of the many units that make up the Twenty-Fourth Air Force is the 561st Network Operating Squadron at Peterson AFB, Colorado. Its crews of operators in a room full of computers keep a close watch on Air Force systems at 108 bases around the world. They work to help repel the more than 1 million attacks against Air Force networks each day.



Members of the 561st Network Operating Squadron work to defend and protect Air Force computers.

Airman 1st Class Dennis Hoffman/Courtesy US Air Force

Air Force JROTC cadets from Spokane, Washington, participate in the CyberPatriot IV competition at National Harbor, Maryland, in March 2012.

Airman 1st Class Alexander W. Riedel/Courtesy US Air Force

The CyberPatriot Program

In the end, protecting computer networks and systems is the responsibility of everyone who uses a computer. In 2009, seeing the need for more young people to be trained in cybersecurity, the Air Force Association (AFA) started the CyberPatriot program. The AFA is a nonprofit independent organization that unites current and former Airmen to promote understanding of airpower and its role in national security.

CyberPatriot conducts the National Youth Cyber Defense Competition. Teams of high school and middle school students compete to manage the network of a small company. They look for holes in cybersecurity and work to plug them while keeping services up and running. Regional winners go to Baltimore, Maryland, for the National Finals Competition.

Another activity of CyberPatriot is AFA CyberCamps, where students like you can learn the importance of cybersecurity and how to protect their personal devices and information from outside threats. Many Air Force JROTC cadets have participated in CyberPatriot events. You can learn more about the program at *www.uscyberpatriot.org*.

In this book, you're read about the history of aviation and the development of airpower. You read how the imaginative thinking of Leonardo da Vinci led people in following centuries to experiment with parachutes and gliders. You read about the Wright brothers' experiments that led to the first controlled, manned, heavier-than-air flight. You studied how aviation developed rapidly during World War I, how Charles Lindbergh captured imaginations with his trans-Atlantic solo flight, and how brave Allied flyers helped liberate Europe and the Pacific region in World War II. You read about the birth of the independent Air Force and the role airpower has played in US global interventions since then. Finally, you explored a bit the new world of cyberspace and the challenges it presents for defending the homeland.

Before you, as before no other generation in the history of mankind, the future of aviation and airpower lies bright with promise and possibilities. Will you be part of it?

✔ CHECKPOINTS

Lesson 3 Review

1. What is the F-35 an unprecedented attempt to do?
2. What kind of aircraft will the KC-46A be able to refuel?
3. Who developed the ARPANET?
4. What is a software patch?
5. Who can cyberspace attackers be? Which is the greatest threat?
6. Where is Air Force Cyber Command located?

APPLYING YOUR LEARNING

7. Explain some actions you can take to make the computers and devices you use more secure.

This page not used