Week 3

Lesson 3: Cyber Security — Is cyber security a key component of our nation's homeland security?

In lessons 1 and 2, you learned about the differences between cyber security and cyber safety. While cyber safety focuses on protecting you, the individual, cyber security is concerned about protecting those things that belong to you, such as your bank account information and social security number. In the last lesson, which focused on cyber security, you learned ways to ensure you don't become a victim of financial crimes.This lesson will focus on cyber security, cyber spying and cyber attacks that pose a threat to our entire nation.

✔ Read the articles *Chinese hackers seek U.S. access* and *Nato to study defense against Cyberattacks*.

Discussion:

◆ What is "cyberwarfare"? What steps is the U.S. taking to combat information warfare attacks from international cyber criminals?

◆ How are Chinese hackers using traditional hacking methods in more and more sophisticated ways? What threats do their activities pose to the USA's national security?

◆ How is NATO working to protect its 26 member nations from cyberattacks? Why did the cyberattack in Estonia this year attract international attention? That is, why was it a wake-up call for governments to take further action to protect against future cyberattacks?

Activity:

1. General Ronald Keys, commander of Air Combat Command, asserts that it's going to take a catastrophic Internet event for the U.S. to seriously re-examine its approach to cyberwarfare. While NATO spokesman James Appathurai believes that "urgent work is needed to enhance the ability to protect information systems of critical importance. In small groups, adopt the role of NATO defense ministers.

2. As a group, define what "information systems of critical importance" are. Then, determine what conditions or what type of cyber attack would grab the nation's attention and cause this country to rethink its approach to cyberwarfare.

3. Use information from the articles and your knowledge of cyber safety and cyber security to draft a five-point plan aimed at dramatically improving the security of the USA's critical information systems, increasing the government's involvement in reducing cybercrime and cyberattacks, and catching and prosecuting cybercriminals. (Remember: Since cybercriminals cross international boundaries, your plan must enlist the help and cooperation of nations in order for any actions to be successful.)

4. Present your plan to the class.

5. After all groups have delivered their presentations, discuss the different approaches that students proposed for combating cyberwarfare. Come to a consensus on a five-point plan that includes the best strategies from each group.

Week 3

Cyber Security — Is cyber security a key component of our nation's homeland security?

Chinese hackers seek U.S. access

Attacks highlight weaknesses in Internet security

By Jon Swartz
USA TODAY

SAN FRANCISCO — The cyberattack of a U.S. military computer system has deepened concern about cyberspying and the security of the Internet's infrastructure.

Chinese hackers were most likely behind an intrusion in November that disabled the Naval War College's network, forcing it to disconnect from the Internet for several weeks, says Lt. Cmdr. Doug Gabos, a spokesman for the Navy Cyber Defense Operations Command in Norfolk, Va.

Forensic analysis indicates the hackers may have sought information on war games in development at the naval college, he said. The college was vulnerable because it did not have the latest security protections, Gabos said.

The November attack was part of an ongoing campaign by Chinese hackers to penetrate government computers. The attacks often come in the form of "spear phishing," scams where attackers craft e-mail messages that seem to originate from the recipient's organization in a ploy to gain unauthorized access to confidential data.

China is also using more traditional hacking methods, such as computer viruses and worms, but in sophisticated ways, says Alan Paller, director of the security research organization SANS Institute.

Hackers are directly breaking into military and government computers, and exploiting the side doors of private networks connected to them, Paller says.

The intrusions spotlight the soft underbelly in U.S. cybersecurity. They also underline the need for the federal government to develop policies that define responsibilities between the public and private sectors to fend off hackers and terrorists, say military officials and cybersecurity experts including Jody Westby, CEO of Global Cyber Risk.

The attacks also underscore flaws in Internet security and the difficulty in tracking bad guys, says Westby, a cybersecurity consultant in Washington. Such "Swiss cheese" holes, she says, not only compromise military and government networks but those of businesses and critical infrastructure.

"The Internet was not designed for security, and there are 243 countries connected to the Internet," says Westby, who estimates 100 countries are planning infowar capabilities. "What's more, many countries don't have cybercrime laws."

Chinese hackers gained notoriety in the USA after a series of coordinated attacks on American computer systems at NASA and Sandia National Laboratories, dating to 2003, were traced to a team of researchers in Guangdong province. The program, called Titan Rain by the Defense Department, first became public in August 2005. The Defense Department has since retitled the program under a classified name.

The hackers are still active, but Gabos would not say if the intrusion at the Naval War College was linked to previous attacks.

China is aggressively improving its information warfare capabilities, according to a December 2006 Chinese military white paper. Its goal is to be "capable of winning informationized wars" by the mid-21st century.

The motives of Chinese hackers run the gamut from intelligence gathering to technology theft and the infiltration of defense networks for future action, cybersecurity experts say.

The intent of Chinese operatives is unclear, but most agree they are gathering information, says Peter Neumann, a scientist at SRI International, a non-profit research institute.

AS SEEN IN USA TODAY MARCH 12, 2007

U.S. cyberwarfare strategy, meanwhile, is disjointed because organizations responsible for cyberoffense, such as the National Security Agency, and defense, such as the Naval Network Warfare Command, are not linked, Gen. James Cartwright, commander of the Strategic Command, said in a speech at the Air Warfare Symposium in Florida in February.

The U.S. must take aggressive measures against foreign hackers and websites that help others attack government systems, Gen. Ronald Keys, commander of Air Combat Command, told reporters in Florida on Feb. 9.

"I think it's going to take an Internet 9/11, and we've had some pretty serious problems on the Internet" for the country to seriously re-examine its approach to cyberwarfare, he said, according to a transcript.

NATO to study defense against cyberattacks

Computer assault staggered Estonia

By Jim Michaels
USA TODAY

BRUSSELS — NATO defense ministers are considering extending the alliance's protection into cyberspace in the wake of a devastating digital attack that nearly crippled member nation Estonia.

Defense ministers agreed "urgent work is needed to enhance the ability to protect information systems of critical importance," NATO spokesman James Appathurai said Thursday.

NATO will begin examining how it may protect its 26 member states from electronic attacks like the one in Estonia, Appathurai said during a meeting of the ministers.

Defense Secretary Robert Gates and a number of the other officials have backed the move to study the issue. No decision has been reached on anything beyond study.

The issue is tricky for NATO. The attacks on Estonia were launched against public cyberspace that controls banking, e-mail and other functions and not the country's military command and control system. The attacks, which began in April and peaked last month, were launched from computers in about 50 countries, NATO spokesman Robert Pszczel said.

The alliance, a product of the Cold War, is based largely on the notion that an attack on one member is considered an attack on all.

The cyberattacks in Estonia, a former part of the Soviet Union, followed its decision to transfer a World War II-era statue of a Soviet Union soldier from a park to a military cemetery. The move triggered riots among Estonia's ethnic Russian population.

The Estonia attacks were "sustained" and "coordinated," Appathurai said.

Estonia bills itself as one of the most advanced nations when it comes to online services. Estonians can vote online, and a large percentage of people there use the Internet for banking and other services.

NATO dispatched a team of specialists to Estonia after the attacks, but it has limited capacity to support broader cyberspace defense efforts.

NATO's capabilities are directed toward protecting the alliance's own network, said Sheena Carrigan, a NATO spokeswoman. Expanding that mission would be up to the alliance's political leadership, she said.