WAR GAMES
AT NAVY SCHOOL

The Naval Postgraduate School is one of several universities linked via the Internet to practice cyberwar against one another. Today is the last day of the two-week exercise. Kandy Phan, left, a civilian on SFS Scholarship Program and Air Force 2nd Lt. Amanda Kelly, right, work on the computers.

By KEVIN HOWE
lhowe@montereyherald.com

Soldiers prepare for battle by simulating on maneuvers.

When the battlefield is cyberspace, though, wars are fought with computer screens, modems, keyboards and software.

On Thursday, 39 students at the Naval Postgraduate School came in from the cyberspace maneuver grounds after four days of mock Internet warfare that pitted a "blue" (defender) team against a "red" (aggressor) team made up of the Army's Land Information Warfare unit and the Air Force's 92nd Aggressor Squadron.

The object of the exercise is for each side to try to penetrate the other's computer systems, aiming to infect them with viruses, shut them down or take

them over.

It's a voluntary, ungraded course for students already immersed in a heavy curriculum of coursework and thesis research, but it's "one of the fun things we do, actually going into and defending systems," said Peter Denning, chairman of the NFS computer science department.

"Otherwise computer security study is a pretty theoretical exercise."

The idea of cyberwarfare has gone beyond theory.

The Naval Postgraduate School's own computer system takes thousands of hostile "hits" each year, said John Fulp, a lecturer in the computer science department and faculty director of the cyberwar exercise.

Army Reserve Maj. Erik Bauder took his annual training as a referee for the cyberwar exercise, now in its third year.

There are probes and intrusion attempts in Department of Defense Web sites all the time, he said, and his unit, the Western Information Operations Center and the Land Information Warfare unit, work at detecting, preventing and tracing them back to their sources, often other countries.

"We get probes all the time," said Cynthia Irvine, an associate professor of the computer science department's Center for Information Assurance and Information Security Studies and Research.

The annual cyberwar exercises are meant to teach students about generic types of attacks and how to deal with them, she said. All sides have a level playing field, using the same free software available over the Internet.

"It's an asymmetric problem," Irvine said. "The defender has to make sure everything is defended. The attacker only needs to find one thing."

The mock war in cyberspace draws students "who are interested in what a real-world situation is," said Marine Corps Capt. Eric Walters, an

CONTINUE ON BACK

Please see Cyberwar page B2
Cyberwar

From page B1

information technology major at the school who led the Navy school team this year.

Like others, he participated in last year's computer warfare exercise "and learned a lot," he said, adding that the work has been closely related to his own thesis, which deals with how people can analyze the vulnerability of computer networks.

Some of the team members are military officers enrolled in various information technology classes, others are civilians enrolled in the National Science Foundation's federal Cyber Service Corps scholarship program, which began in 2001.

That program offers a two-year, full-ride scholarship in a computer science master's degree program aimed at safeguarding computer systems, with fully paid tuition, an annual housing and meal stipend and placement in paid summer internships with government agencies.

Graduates are expected to serve two years with a U.S. government agency as specialists in safeguarding computer systems.

Cyber Corps student Jessica Murray, 23, came to NPS after graduating with a degree in computer science from the University of Michigan and is due to graduate in June.

Her project is developing a "back door" to Microsoft XP to demonstrate that system's vulnerability to insider sabotage and to develop techniques to reduce that threat.

"I spent a lot of time" on the 2002 cyberwar exercise, she said, to the detriment of her classes, but the experience piqued her interest in computer security and fit with her thesis.

She has a job lined up after graduation, but she can't say where.

Army Reserve Sgt. Reggie Lewis of Modesto, also with the Western Information Operations Center and a referee, said he was impressed with the level of expertise shown by the students. He will rehash the action with them to show where he detected intrusions and critique how they reacted to them.

"The Red Team," he added, "was largely unsuccessful. It was a validation of the prehardening of the system that they were unable to penetrate it."

The team spent four days, eight to 12 hours a day, at their computers during the actual attack, while the preliminary work setting up the Internet battlefield consumed about two months, Fulp said.

He said it will be some weeks before anyone knows who won.

Kevin Howe can be reached at 646-4416.