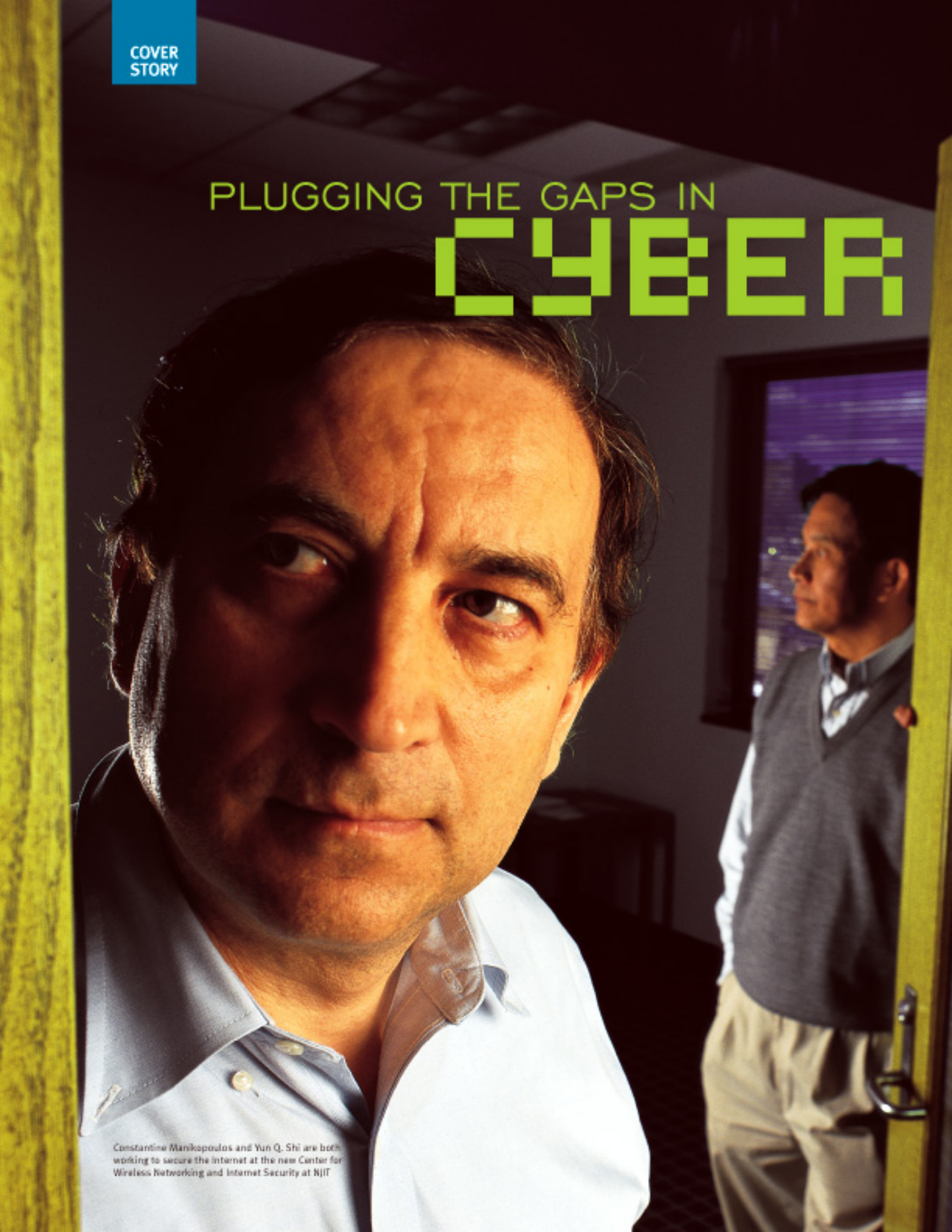


COVER
STORY

PLUGGING THE GAPS IN

CYBER



Constantine Manikopoulos and Yun Q. Shi are both working to secure the Internet at the new Center for Wireless Networking and Internet Security at NJIT

SECURITY

AUTHOR: S. J. LADD is a New Jersey-based freelance writer who specializes in a wide range of technology and business issues.

THE HONKER UNION OF CHINA HACKED INTO MORE THAN EIGHTY UNITED STATES GOVERNMENT WEB SITES LAST SPRING, DEFACING AND CRIPPLING THEM WITH SEEMINGLY LITTLE EFFORT. IT WAS PART OF AN ORGANIZED RESPONSE TO THE DEATH OF WANG WEI, THE CHINESE PILOT DOWNED IN A COLLISION WITH A U.S. SPY PLANE. ALTHOUGH LITTLE PERMANENT DAMAGE WAS DONE, THE INCIDENT IS A CHILLING REMINDER OF THE GAPING HOLES IN CYBER SECURITY THAT ARE NOW CONSIDERED A NATIONAL THREAT. IT IS THE SORT OF THREAT THAT RICHARD CLARKE, PRESIDENT BUSH'S CYBER SECURITY CZAR, HAS CALLED A POTENTIAL "DIGITAL PEARL HARBOR."

"Our nation barely recognizes the extent of its cyber vulnerability," warns Constantine Manikopoulos, intrusion detection expert and associate professor in the Department of Electrical and Computer Engineering (E.C.E.). "Many utility, corporate and government networks are linked by the Internet. Theoretically, if one is attacked, a whole series of infrastructures can be attacked," he continued. "We haven't seen anything yet."

He should know. Manikopoulos is part of a team of NJIT researchers led by Atam Dhawan, E.C.E. professor and department chairman, working to bolster national cyber security at the Center for Wireless Networking and Internet Security, a major research effort that was launched at NJIT last December through a five-year, \$2.6 million grant from the New Jersey Commission on Science and Technology. Dhawan is the director of the center, run jointly by NJIT and Princeton University. Center researchers are investigating methods of predicting cyber attacks, identifying data senders and receivers, creating secure battlefield networks, developing new

techniques for recovering damaged digital data and improving the security of wireless connections to the Internet. Until the World Trade Center attack on September 11, such projects received little attention.

"We were the ugly step-sister," said Manikopoulos, comparing security studies to well-funded research that produced popular wireless technologies such as palm-held computers like personal directory assistants (P.D.A.s). "Until now, the bigger concerns have been providing more features and better functionality – not security." As a result, the nation became highly vulnerable as wireless technology spread into e-commerce, health care, inventory control and other on-line communications, noted Dhawan. "Security controls haven't kept pace with change," he said. For example, wireless networks use encryption codes to combat access to classified cyberspace information like credit card numbers and trade secrets. But last year, California researchers cracked the most popular encryption system.

One of the most common types of Internet terrorism is a distributed Denial of Service (D.O.S.) attack. D.O.S. attackers remotely commandeer hundreds of Internet-connected personal computers and use them to release a disabling deluge of data against a web site. Like gas mask-wearing robbers who release tear gas in a bank, web intruders can pick their way through the confusion to work their mischief while legitimate users are denied access.

Manikopoulos, who worked five years on a U.S. Army anti-intrusion project, is designing strategies for predicting attacks of all kinds. Attackers, he explained, leave clues.

Like criminologists, intrusion investigators pore over computer records of past attacks to find these clues. Researchers catalog the idiosyncrasies, or anomalies, as Manikopoulos calls them, in network databases. By using probability equations and other techniques, he can estimate the potential for recurrence.

"By searching the system and matching it with the data, you sometimes can figure out what's happening even before an attack actually begins," he said.

So far, this work has been based on a body of knowledge derived from prior attacks. The main research challenge now, said Manikopoulos, is to identify attacks for which there is no precedent.

"Of course, this will be much harder," he said. "But we think it is possible."

Dhawan is investigating signal-processing systems for protecting digital data through improved coding. His field, digital watermarking, relies on mathematical coding to deliver images and audio signals. It is best known for embedding hidden information to protect on-line music recordings. While encryption ensures only authorized users can see files, watermarking offers additional information that assures correct, uncorrupted data.

Dhawan is experimenting with a set of mathematical functions called wavelets, used in compressing bulky still-image or video files for quick computer

DO YOU FEEL SAFE?

The latest data from a January NJIT tech poll reveals what people in New Jersey really think about the state of technology and safety. Four hundred people were asked more than fifty questions about safety. Here's a sample of questions and answers.

Note that percentages have been rounded and therefore may not add up to one hundred.

- 1.** Would you say computer systems and the Internet are more secure from attack by terrorists or hackers since September 11?

 - 6% Much more secure
 - 17% Somewhat more secure
 - 11% Somewhat less secure
 - 6% Much less secure
 - 39% No change
 - 20% Don't know/refused
- 2.** To promote safety and security, is it a good idea to use computer technology to scan for the faces of criminal or terrorist suspects in public places such as airports and stadiums?

 - 45% Excellent idea
 - 39% Good idea
 - 9% Only a fair idea
 - 6% Poor idea
 - 1% Don't know/refused
- 3.** To promote safety and security, is it a good idea to increase the use of computer programs that create profiles of people considered a risk based on their behavior, including those who travel to unfriendly countries or use cash for purchases of things such as airline tickets or cars?

 - 30% Excellent idea
 - 37% Good idea
 - 15% Only a fair idea
 - 15% Poor idea
 - 4% Don't know/refused

downloading. In the process he is designing, images are sent in several pieces at various spectral – or light – frequencies, some of them not normally used for data transmission. To enhance security, each piece receives a special watermark in a process called multilevel dynamic coding.

A second marking project led by Yun Q. Shi, E.C.E. associate professor, also holds great promise. Shi, active for four years in the field of multimedia watermarking, is trying to make the process less vulnerable to corruption. One of his initiatives would improve the technique of interleaving – scrambling the order in which codes for speech and video data are received.

Crude, highly adverse conditions, such as battlegrounds or disaster sites, present a formidable challenge for secure communications. Symeon Papavassiliou, E.C.E. assistant professor, is attempting to design Internet-like, wireless subsystems that will offer this unexpected ability even when sites have not been prepared for secure telecommunications. Called mobile ad-hoc wireless networks, they will depend simply on a portable computer.

"What makes this so difficult is that there's no fixed infrastructure," said the researcher, "so we have to create one – spontaneously."

Under normal conditions, a complete, functional wireless network requires nodes, or traffic centers, to be in place to route communications from one user to another. Without nodes, a network simply cannot operate. Each of these traffic centers also

ALUMNI WATCH



HOMEGROWN NATIONAL SECURITY EXPERT

Jim Lindenfelser '64 takes national security issues in stride. He leads a team of highly cleared engineers, computer scientists, ana-

lysts and telecommunications engineers who provide the computer and telecommunications security expertise critical to national defense and operations around the globe. His main clients are national security organizations of the federal government. Senior vice president and director of the Space and Communications Operating Unit at TASC, a subsidiary of Northrop Grumman, he also spent twenty-two years in the United States Air Force. "My whole career has been security focused," he remarked.

His group at TASC offers a special service known as InfoShield™, which provides an assessment of the vulnerability of an enterprise to cyber attack. It can also redesign a network to eliminate or reduce vulnerability. Lindenfelser, who has been involved with InfoShield since its inception, describes it as "a living product that we continuously improve."

Lindenfelser is also responsible for a state-of-the-art laboratory where new technologies for cyber and physical security are developed and tested. Lab researchers work under his guidance, and he establishes investment priorities.

In his State of the Union address last January, President Bush asked citizens to give two years of service to the country. It appears that Lindenfelser has more than satisfied this requirement: he has given his entire career.

— Johanna R. Ginsberg

4. To promote safety and security, is it a good idea to use retinal scanners that will recognize patterns in the eye to verify a person's identity before allowing them to use an ATM?

33% Excellent idea
33% Good idea
16% Only a fair idea
15% Poor idea
2% Don't know/refused

5. To promote safety and security, is it a good idea to use retinal scanners that will recognize patterns in the eye to verify a person's identity before allowing them to board a plane?

45% Excellent idea
33% Good idea
12% Only a fair idea
9% Poor idea
1% Don't know/refused

6. Some people say more emphasis should be placed on stopping terrorism and criminal activity by increasing human intelligence, such as gathering better information by having more intelligence agents on the ground overseas and by training law enforcement, baggage handlers and others to be more vigilant. Others say that we should instead rely on technology by using facial recognition systems at airports, having computers do behavior profiling and improve

scanning technology at airports, mail facilities and public places. Which view comes closest to your own?

32% We should rely more on human intelligence
18% We should rely more on technology
47% We should rely on both equally
1% Neither
1% Don't know/refused

must be capable of accepting and relaying multiple transmissions simultaneously. In addition, each must be able to sense security intrusions.

The solution, said Papavassiliou, involves organizing several highly sophisticated mobile nodes inside the mobile network group, some assigned to stationary or slow-moving users and others assigned to fast-moving users. Each would be equipped to route wireless communications among users as they move in and out of the immediate region while simultaneously sensing potential intrusions.

Solving the ad-hoc network's complicated technical problems relies on a cross-disciplinary approach. Manikopoulos, for example, is contributing his anti-intrusion strategies. E.C.E. assistant professor Sirin Tekinay, who specializes in network management,

Attackers leave clues. Like criminologists, intrusion investigators pore over computer records of past attacks to find these clues [and] estimate the potential for recurrence. The challenge now is to identify attacks for which there is no precedent. Of course, that will be much harder, but we think it's possible.

is designing wireless systems for pinpointing the locations of each mobile user, both inside and outside the ad-hoc network.

Actually, Tekinay's overall research project extends well beyond the mini-network. She is studying strategies for locating users and disseminating information to and from them throughout the world.

She summed up her research goal in a simple phrase – “anyhow access” – and she used her own situation to describe its potential. “I should be able to access anything I need on the NJIT network with an appropriate level of security whether I’m on the go, in the office or at home,” she said.

Such seamless global access now is impossible for two main reasons. First, wireless carriers in the United States and the rest of the world have adopted technical communications standards and protocols that are incompatible with one another.

Second, the transmission capacity – or bandwidth – for funneling digital data over the airwaves to mobile computer equipment is much more limited than the huge bandwidth provided by wired systems; transmission is also more fragile, particularly as a user moves from cell to cell and tries to download bulky files.

To tackle the standards issue, Tekinay is leading the center's effort to persuade the international standards-setting agencies to include consistent and appropriate security protocols in the design of the next – or fourth – generation of wireless protocols.

As for capacity issues, she is suggesting alternatives. One involves designing methods for bypassing wireless technology altogether. Another would encourage wireless carriers to recognize usage in addition to location in granting or denying authorized access to restricted data.

One recommendation calls for wired Information Stations to be installed at airports and other convenient locations. These stations would provide access to the Internet for downloading at high speed, for example, without wireless bandwidth complications. For times when stations are unavailable, Tekinay is suggesting wireless methods for distinguishing among computer devices, and the ways they are being used, to determine access.

Industry leaders are closely watching the progress of all these initiatives, especially their wireless applications. For Kevin Carswell '79, vice president of worldwide hard disk drive development at IBM, managing security is a crucial step in the promising future of a field that many believe may someday dominate every level of commerce.

“The structured focus on management and security of complex wireless networks is absolutely needed,” said Carswell, whose Fortune 500 company is reviewing the center's projects. “Wireless is growing so quickly that soon almost everything will be hooked to the Internet through the airwaves – data phones, P.D.A.s, cars, even vending machines that automatically call up distributors to tell them they're out of soda.”

No matter how good our research is, though, warns Tekinay, “we will always face some risk. The most secure network is one in which no one communicates with anyone.” ■

BIOMETRICS RESEARCH COULD THWART HIJACKERS

When planes crashed into the World Trade Center on September 11, many travelers asked why science had not yet developed a technology that allows ground personnel to seize control of a hijacked plane. When they saw televised videotapes of the hijackers taken by airport security cameras a few days later, many also wondered why face recognition technology could not be used to identify the terrorists before they boarded the planes.

Questions like these have long challenged researchers working in the field of biometrics, the science of identifying people by measuring and classifying their unique physical characteristics, such as the ridges and grooves on fingers, the iris of the eye and the contours and wrinkles of the face. For two biometrics researchers at NJIT – face recognition expert Chengjun Liu and hand grip specialist Michael Recce – the persistent questions spawned by the terrorist attacks have helped focus attention on some highly promising research.

To Recce, director of NJIT's Center for Computational Biology and Bioengineering, and Liu, assistant professor in the new College of Computing Sciences, the human body literally holds the key to the age-old dilemma of restricting access to a limited number of people.

"A traditional key, even an electronic key, can be lost, stolen or duplicated," observed Recce.

"But each one of us has only one face," said Liu. "You carry it with you everywhere."

Indeed, the faces of some of the September 11 terrorists had already been placed on the FBI's Most Wanted list and theoretically could have been matched with the videotaped images captured at the airports. Such a system is not in effect, however, and for good cause, said Liu who has been working in the field for six years. While a graduate student at George Mason University, he was involved in the development of a government-sponsored face recognition database that has become the de facto standard used to test face recognition algorithms around the world.

Research has shown, however, that the technology's reliability declines over time, partly because the database must be continually updated to accurately correspond with facial changes caused by aging and cosmetic alteration. Lighting conditions for cameras strategically located in public places, such as airports, also produce images that frequently do not clearly match those in the database, he said.

"Technology is not ready yet to solve all the problems," Liu noted.

Nevertheless, accuracy has improved significantly through his image encoding and classification research, which takes into account factors such as emotional reaction and variations in illumination. Liu, who is expected to publish

his findings in March, has applied for a patent to protect his process.

Recce, who is developing electronic sensors in a gun handle to authenticate firearm users, has also applied for a patent to adapt his hand grip technology for use by airplane pilots. His initial research focused solely on the placement of tiny sensors to ensure that the electronic "smart gun" would operate only for those authorized to use the weapon. (See *NJIT Magazine* Fall 2000.)



But his experiences in Manhattan on September 11 prompted him to expand the horizon of his research.

"I saw each of the Twin Towers collapse," said Recce, who wore shoes covered with dust from the disaster for several days. "I was very upset, of course. Later, I got to thinking about how the tragedy could have been prevented, and it occurred to me that hand grip technology might be an answer."

Since operation of modern aircraft frequently shifts between the pilot and ground controllers, Recce reasoned that the installation of his grip sensors in the cockpit controls could be achieved with relative ease. Only the authenticated grips of the pilot or copilot would be programmed to operate the plane.

"When the pilot releases his or her grip, control of the plane would revert to the ground," he said. "A terrorist couldn't pilot the plane."

With some adjustments in the design of the aircraft, ground controllers could even land the plane, as they often do with aircraft carrier planes, he added.

— S. J. LADD