

CAPABILITIES FOR THE ARMY'S FUTURE FORCE¹⁰

The Army's Future Force¹¹ is literally the future Army, with transformational changes required in the areas of leader development, acquisition, training, sustainment, and institutional initiatives. Central to the Future Force is the concept of network-centric warfare (NCW).

NCW is intended to provide three fundamental capabilities to the warfighter and his or her commander through real-time networking. NCW shifts the emphasis from platform-based to network-based capabilities, thereby generating the following opportunities:

- *All members of the network will have access to all networked resources within established security protocols.* Even single platforms can access all of the resources residing within the network. These resources include the sharing of situational awareness with all members of the network, so that all NCW participants can immediately see the whole battlefield.
- *Networked commanders can make more informed decisions.* The commander of an NCW force is able to see the whole picture from the viewpoint of any member of his or her network. The commander is thus able to understand the entire situation quickly.
- *A networked force can more effectively and efficiently synchronize its assets.*

NCW provides commanders with the capability to generate precise warfighting effects at an unprecedented operational tempo, creating conditions for the rapid countering of adversary courses of action. As a result, operations may become more efficient and the conduct of war may change. For example, close air support operations may be significantly reduced by the increased ability to anticipate the need for air support and thus to avoid or minimize situations that involve a time-critical requirement for conducting air operations in close proximity to friendly forces.

It is anticipated that, just as NCW acts as a force multiplier on the battlefield, network-centric operations (NCO) could benefit homeland security. While some of the capabilities that are being developed for the Future Force might be too complex or expensive for the use of emergency responders, many of the technologies would be very helpful, and the concept of network-centric operations could provide a common framework for these technologies.

¹⁰ Army Science and Technology for Homeland Security: Report 2 -- C4ISR. Copyright 2004 © National Academy of Sciences.

¹¹ The Future Force (previously called the Objective Force) is the force that the Army is planning for its future. The Future Combat System (FCS) is envisioned as being one of several yet-to-be determined systems that will be part of the Future Force.

Army of the Future.. G.I. Dot Joe

THE CONTEXT AND PURPOSE OF our military forces is changing—from fighting grand wars like World War II, to engaging in smaller, focused conflicts and more peacekeeping missions like Kosovo or Afghanistan. The joint forces of tomorrow must not only be prepared to meet armies on the battlefield, but to meet rogue combatants in complex, populated urban landscapes. They must be able to withstand not only major artillery, but a broader spectrum of nontraditional threats such as chemical, biological, and cyber attacks. And they must do all this while keeping both civilian and our own casualties to an absolute minimum.

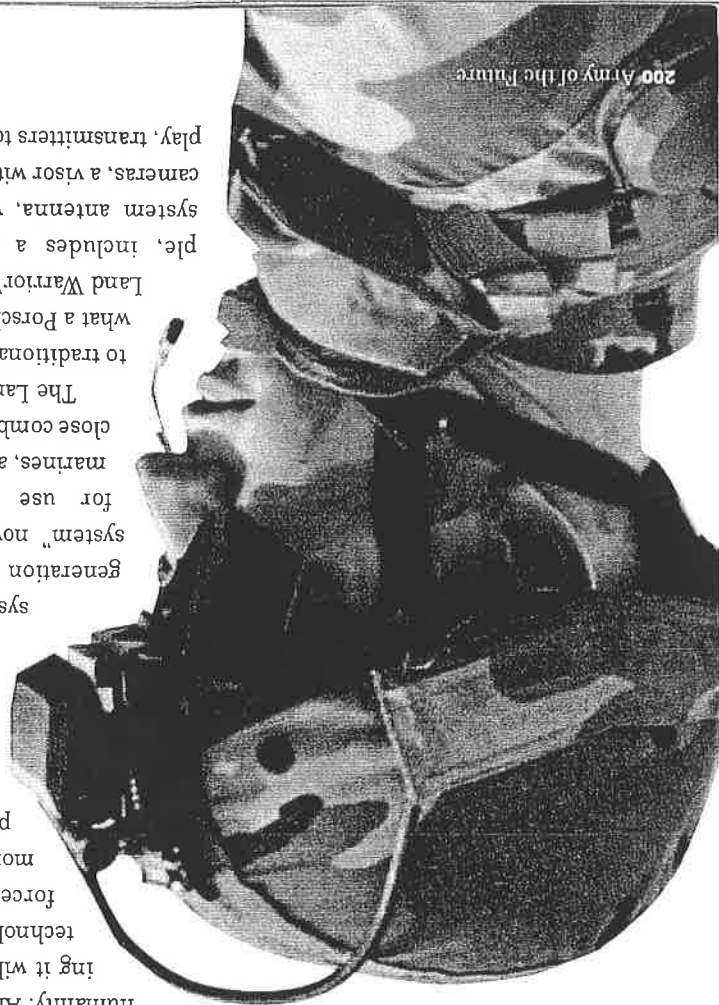
as an American to other fighters, as well as chemical and biological weapons detectors and a gas mask. An integrated mic, radio, and wireless LAN devices allow each soldier to know the precise locations of fellow soldiers, enemies, and targets; let soldiers see real-time maps of the battlefield terrain; and allow commanders to send text messages to each soldier's helmet-mounted displays.



The Land Warrior system is close combat. for use by the infantry, marines, and other soldiers in the development of the Land Warrior system, the next-generation "individual fighting system" now being prototyped for use by the infantry, marines, and other soldiers in close combat.

A major step forward toward full-filling this vision is the development of the Land Warrior system, the next-generation "individual fighting system" now being prototyped for use by the infantry, marines, and other soldiers in close combat.

That's the tallest order ever given to any fighting force in the history of humanity. And the key to fulfilling it will be the use of new technologies that make our forces smarter, faster, more lethal, and more precise.



THE LAND WARRIOR SYSTEM. The fighting fatigue of tomorrow.





The protective clothing and individual equipment subsystem incorporate modular body armor and upgrade plates that can stop small-arms rounds fired at point-blank range. It includes chemical/biological protective garments and is 35% lighter than traditional "flak jackets."

The weapons system is built around the traditional M-16 but includes a host of advances, including a laser range finder, a digital compass, a thermal sight, and a daylight video sight — an attached camera that not only allows soldiers to literally "shoot around corners," but to take pictures that are relayed to other soldiers in the field.

Future enhancements to the Land Warrior system will include thermal controls that allow soldiers to maintain their body temperature in extreme environments and built-in medical sensors that allow commanders and remote medics to check on a soldier's vital signs with the push of a button.

These technologies don't just make soldiers more effective and immune to killing machines — they actually change the nature of military actions. They allow for more distributed, real-time decision making by forces on the ground, and allow individual soldiers to better understand the behavior of their entire platoon. A new kind of "swarm" behavior emerges, as the soldiers, both peers and commanders, can take advantage of massive amounts of information in real-time.

The cost of the Land Warrior system is kept low by using off-the-shelf technologies whenever possible. Each Land Warrior is powered by ruggedized off-the-shelf technologies including a Pentium processor and Windows operating system. The program will cost \$2 billion when 45,000 sets of the equipment are fielded over the next 15 years.

Land Warrior is just the beginning, however. The military is also just beginning to test a variety of new technologies that will revolutionize every aspect of force deployment. At the Army's Soldier Systems Center, for example, engineers are developing a Transdermal Nutrient Delivery System (TNDS) — a patch that will keep soldiers fed when they are in extreme situations where they can't get a meal for an extended period of time. Like a nicotine patch, the TNDS delivers nutrients directly to the soldier's bloodstream until help arrives.

And at the newly created Institute for Soldier Nanotechnologies at MIT, scientists are exploring the revolutionary applications of nanotechnology to every aspect of soldiering, including the

creation of uniforms that change colors to camouflage the wearer, that provide super-human performance enhancements, and that can become a rigid cast when a soldier breaks his or her leg. While these kinds of technologies are not expected to be fully developed for another 15 years, they point the way to an era when "military intelligence" is no longer dismissed by some as an oxymoron.

PROVOCATIONS...

Will drill sergeants scream at privates to move their joysticks?
Will a dying soldier one day send his spouse instant messages from the battlefield?

—Andrew Zoll

WANT MORE?

SOLDIER SYSTEMS CENTER

www.natick.army.mil

PM SOLDIER SYSTEMS

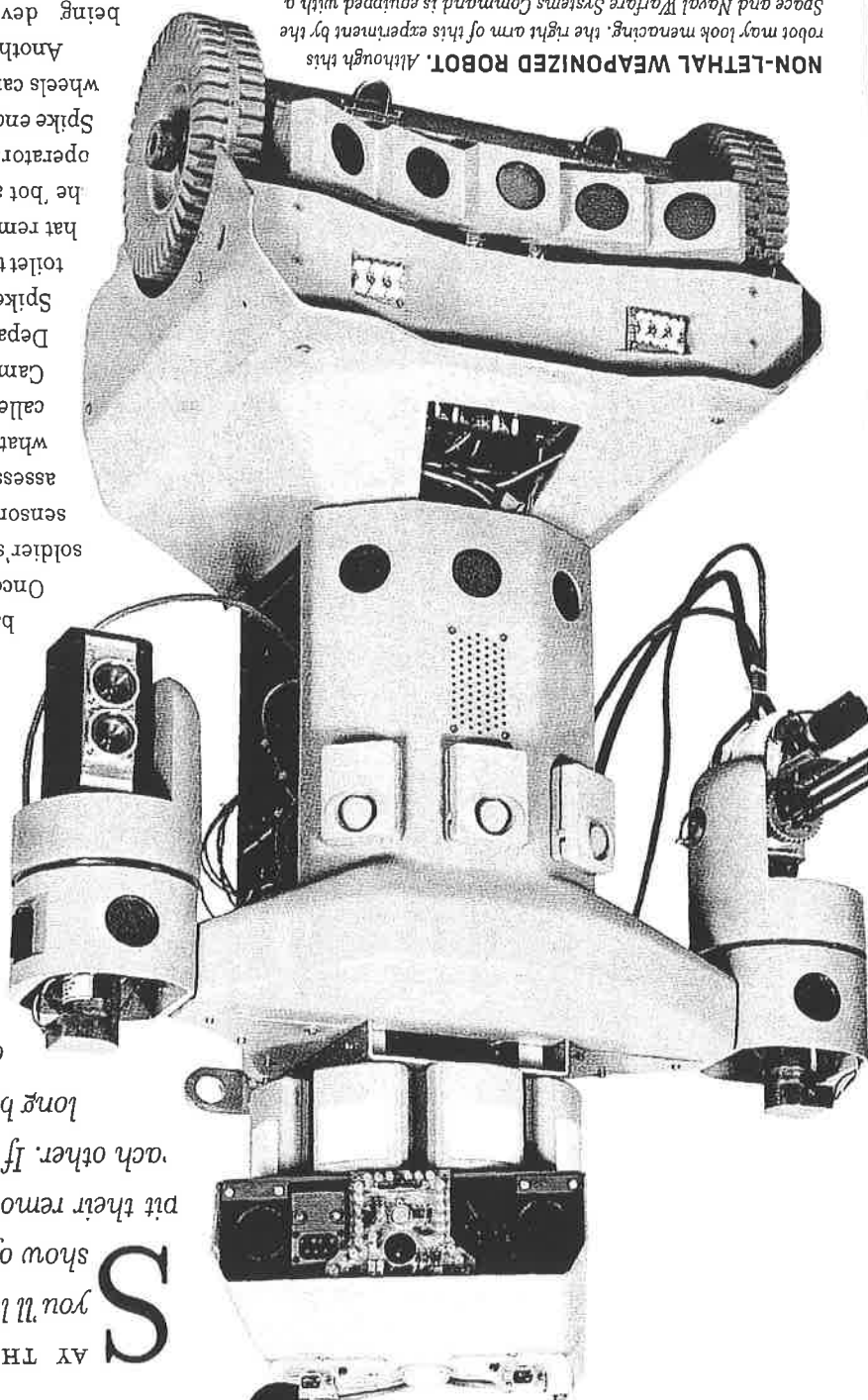
www.pmsoldiersystems.army.mil/

public/default.asp

AMERICA'S ARMY

www.americasarmy.com

NON-LETHAL WEAPONIZED ROBOT. Although this robot may look menacing, the right arm of this experiment by the Space and Naval Warfare Systems Command is equipped with a six-barreled tranquilizing dart gun.



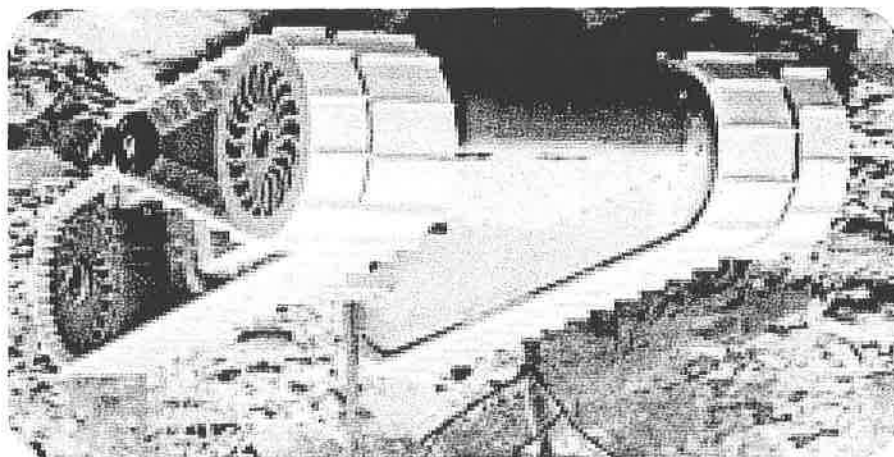
Military Robots...

AT THE WORD "BATTLEBOTS" TODAY AND you'll likely conjure up images of the popular TV show of the same name where teams of players pit their remote-controlled fighting machines against each other. If development proceeds apace, it won't be long before a "battlebot" is something far more ominous, an autonomous robot that can roll onto a battlefield and engage an enemy. Defense developers have a long ways to go before they get to this point, but there have been some recent advances in battlefield robotics that, at least for the moment, are more about helping soldiers than taking lives.

Imagine a robot that a soldier can carry in a backpack and toss through a window like a grenade. Once deployed, the "bot" becomes an extension of the soldier's senses, scouting out enemy units, using special sensors to sniff for biological and chemical weapons, and assessing other 21st-century battlefield hazards. This is what "throwbots" are all about. One such throwbot, called Spike, was developed at Draper Laboratory in Cambridge, Massachusetts, as part of the Defense Department's Tactical Mobile Robots (TMR) program. Spike looks something like the copper float inside your toilet tank. Once tossed, its center expands to form an axle that remains stationary while the half-sphere wheels move the "bot" around. Inside the thick axle is a video camera. An operator, out of harm's way, can see what the robot sees. If Spike encounters rough terrain, such as rubble, a set of spiky wheels can be deployed to give the robot greater traction.

Another type of man-portable robot, called a PackBot, is being developed at iRobot, a company founded by well-known M.I.T. robotics pioneer Rodney Brooks. Looking not

Images courtesy of Space and Naval Warfare Systems Center, San Diego



PACKBOT. Designed to accommodate different types of tactical robot configurations.

PROVOCATIONS...

Will we one-day turn over lethal combat decisions to robotic warriors?

—Gareth Branwyn

WANT MORE?

DOD JOINT ROBOTICS PROGRAM

www.jointrobotics.com

DARPA TACTICAL MOBILE ROBOTS

www.darpa.mil/ato/programs/tmr.htm

DARPA DISTRIBUTED ROBOTICS

www.darpa.mil/mto/drobotics

SPACE AND NAVAL WARFARE

SYSTEMS COMMAND

www.spawar.navy.mil/robots

MOBILE ROBOT DATABASE

<http://robot.spawar.navy.mil/>

MobileRobotKB

IROBOT

www.irobot.com

FUTURE COMBAT SYSTEM

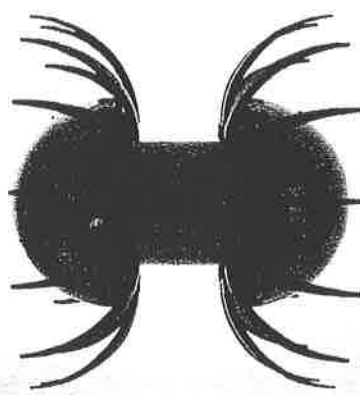
www.darpa.mil/fcs/index.html

SAIC

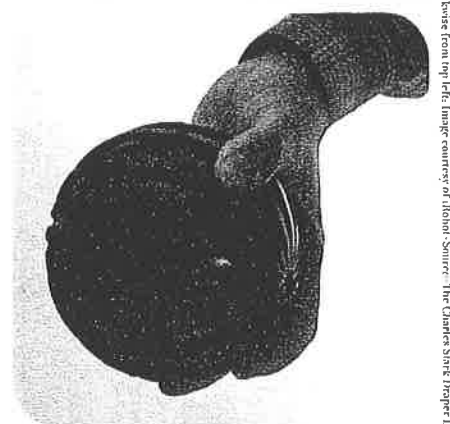
www.saic.com

unlike a remote-controlled kid's toy tank, PackBot is really a platform to accommodate different types of tactical robot configurations. It can be outfitted with numerous environmental sensors, for reconnaissance and threat assessment, and it can be used to haul ordinance or supplies. It's even been tested as a robotic ambulance where, towing a stretcher, it can pull up alongside a wounded soldier who then rolls onto it before being hauled out of harm's way. iRobot is also working on a number of other DoD-funded projects, such as MUMS (Micro Unattended Mobility System), a semi-autonomous 'bot similar to Draper's Spike that can even be fired from a grenade launcher, and Swarm, a project to develop the software needed to coordinate data between distributed groups of autonomous robots. The Tactical Mobile Robot program was hastily put to the test after 9-11. Lt. Col. John Blitch, who had retired as the head of the TMR program the day before the terrorist attacks, quickly assembled a team of operators and 'bots from various TMR developers. Seventeen robots in all (including iRobot's PackBots) worked Ground Zero, searching for survivors. The success of the robot recovery workers at the World Trade Center and

the achievements of the unmanned Predator planes over the skies of Afghanistan have opened many people's eyes to the real-world potential of robotic and tele-operated machines to do what Michael Toscano of the Pentagon's Joint Robotics Program calls the "dirty, dangerous, and dull." While this attention is leading to stepped-up activity in the field, there is still a long way to go before robotic battlefield assistants become commonplace. Wartime periods have a way of accelerating technological innovations, and the war on terrorism is likely no exception, so we may be seeing 'bots on the battlefield sooner than we thought.



THROWBOT. "Spike" extends a soldier's eyes and ears by means of special sensors.



Clickbase from top left: Image courtesy of iRobot. Source: The Charles Stark Draper Laboratory, Inc.

CYBERWAR AND CYBERTERRORISM... DANGER ON THE DESKTOP



ON SEPTEMBER 11, 2001, A SMALL, LOOSELY-ORGANIZED group of terrorists pulled off a sudden, complex attack on the World Trade Center in New York City that killed thousands and caused immediate, radical shifts in many nations' policies. What would be next? Many worry that the encore could be an "electronic Pearl Harbor" as devastating in the digital world as the September 11 attacks were in the physical world. Could terrorists hack into the banking system? The Pentagon? A nuclear power plant? For years, military theorists have looked at how to fight wars in which computer programmers are the generals, laptops the infantry, and software the weapon-

HIDDEN INFORMATION. Before-and-after versions of a drawing of Shakespeare, one normal and one with a steganographic message inserted using a program called White Noise Storm. The images are identical to the unaided eye and serve as a good illustration of how Al Qaeda is alleged to have hidden messages in harmless-looking imagery: **VISUAL ENCRYPTION.** This Al Hirschfeld drawing (top right) of The Bard is a simple example of visual encryption. You should be able to find five instances of "Nina" hidden in this drawing. The Pentagon used Hirschfeld drawings to test acuity in finding targets. Subjects had to identify the NINAs.

ry. They've coined terms like information warfare for the ancient art of using data to gain advantage. Capturing messengers in ancient Greece and breaking Nazi codes were both information warfare; those



AN INFOWAR PRIMER

INFORMATION WARFARE: An umbrella term for any offensive or defensive use of information to shorten your decision-making cycle while disrupting an opponent's. Breaking an enemy's codes is one example.

INFORMATION

DOMINANCE: The achievement of a clearer picture of a battlefield than an opponent has. The combination of satellite photography, drone reconnaissance, and ground observers helped U.S. forces achieve this in Afghanistan.

CYBERWAR: The use of computers and other electronic tools to increase your ability to destroy an opponent or his ability or will to fight. The 1998 NATO campaign against Serbia was partly a cyberwar.

CYBERTERROR:

The use of computer networks to damage physical or information infrastructure and cause fear among a citizenry or government. Cyberterror could range from destruction of bank records to sabotaging computers at a nuclear power plant.



European networks, blurring the "front line" of the conflict.

While cyberwar can be thought of as

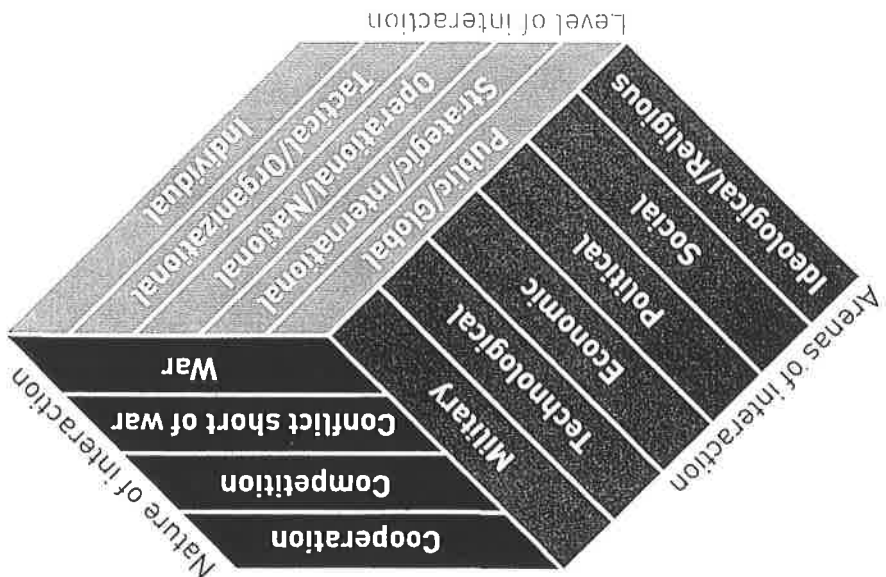
nations fighting nations, cyberterrorism is what non-state groups do to everyone else. Cyberterrorists use technology to generate fear that causes citizens or governments to change their actions and goes far beyond merely jamming an e-commerce site or defacing a government Web page. For example, in 2001, an Australian rejected for a local government job avenged this slight by hacking into the computer that controlled the local sewage system. Using a two-way radio and a laptop, Vitek Boden caused the facility to dump about 1 million liters of sewage onto a nearby resort. "It had very serious

who learned their enemies' secrets could make better, faster decisions and multiply their soldiers' impact.

Cyberwar is a modern subset of information warfare: using computer networks and other electronic tools to

both assess a battlefield and destroy an enemy — or that enemy's will to fight in the first place. NATO's 1998 operation against Serbia is a prime example. The Alliance monitored and disrupted Serbian phone calls, email exchanges, radio and TV transmissions, and computer networks to cripple the Serbian military's confidence in its communications, just as the threat of bombing destroyed its ability to move heavy weapons. Pro-Serbian hackers tried doing the same to U.S. and

Axes of information warfare



SCOPE OF INFOWAR. As David Alberts explains in *Defensive Information Warfare* (1996): "The scope, or battlespace, of information warfare and strategy (IWS) can be defined by the players and three dimensions — the nature of their interactions, the level of their interactions, and the arena of their interactions. Nations or combinations of nation states are not the only players. Non-state actors (including political, ethnic, and religious groups; organized crime; international and transnational organizations; and even individuals empowered by information technology) are able to engage in information attacks and to develop information strategies to achieve their desired ends."

which uses email and cryptography extensively and whose members can act without central direction.

Computer networks enable these small groups to quickly "swarm" at targets via letter-writing campaigns, innovative computer code, or destructive terrorist attacks. The result? Big political and economic impacts from relatively few people. Security experts face the problem of a large-scale network: a decentralized but wired enemy making a coordinated series of electronic feints and punches against business and government, from railway signaling

NETWAR AND "SWARMING"

Some cyberterrorism and cyberwar may also be network, a concept explored and popularized by John Arquilla and David Ronfeldt, in which antagonists use networked organizations and technologies to achieve their goals. Unlike traditional military or business enterprises with their top-down chains of command, these networked organizations may be loosely structured or even leaderless, with members independently pursuing various causes.

Dr. Dorothy Denning, a Georgetown University professor who is a leading computer-security expert, "If Hamas had done that, we would call it terrorism." Could cyberterrorists hack into, say, the air-traffic control system or a nuclear plant? It's possible, just as it's possible they could shoot their way in; computer networks are so complex that they'll always have some vulnerability. But terrorists might rather hack into a company's payroll system or a bank's records.

122° 24' 36" W, 37° 46' 26" N

Most security systems are based on something you know (a password) and perhaps something you have (a passkey or other device). But so-called geolocation, as checked by global positioning system (GPS) signals, this would help verify that you're in a CIA building rather than a Central Asian cave. Beyond worries about Osama bin Laden, geo-encryption could also ensure that a DVD is played only at your home — rather than on the black market — or that your record collection didn't migrate to an online music-sharing operation. The idea has problems, however. The federal government, which operates the GPS network, sometimes degrades the accuracy of commercially available GPS signals from roughly 1-5 meters to as many as 100 — the difference between you logging in on the guy at the phone booth down the block. Also, critics worry about criminals mimicking GPS signals from afar. Even with these problems, some experts believe that "being in the right place at the right time" will soon have a whole new meaning.

WANT MORE?

DEFENSIVE INFORMATION WARFARE, BY DAVID ALBERTS
www.ndu.edu/ndu/inss/books/div/index.html
 DOROTHY DENNING AND
 GEO-ENCRYPTION
www.smartbusinessmag.com/article/0,3658,apn=2&s=101&a=2483
 DENNING'S LINKS
www.cs.georgetown.edu/~denning/links.html
 INFORMATION WARFARE
www.infowar.com
 FED. OF AMERICAN SCIENTISTS
www.fas.org/irp/wwwinfo.html
 RAND ARTICLES
www.rand.org/publications/MR/MR661
www.rand.org/publications/MR/MR789
 "AN ELECTRONIC PEARL HARBOR?"
<http://205.130.85.236/issues/15-1/smith.htm>
 INST. FOR THE ADVANCED STUDY OF INFORMATION WARFARE
www.psych.com.net/iwar.1.html
 INFO WAR SITE
www.iwar.org.uk
 BAN LANDMINES CAMPAIGN
www.icbl.org
 OPEN SOURCE INITIATIVE
www.opensource.org
 OPEN SOURCE DEVELOPMENT NETWORK
www.osdn.com

systems to the computers at the New York Stock Exchange. Such a careful combined attack could generate chaos, forcing the victims to shut down their systems until damage can be assessed. Everyday life could become extremely difficult for awhile. "If they were able to obliterate your bank account, that would seriously scare people," Dorothy Denning says.

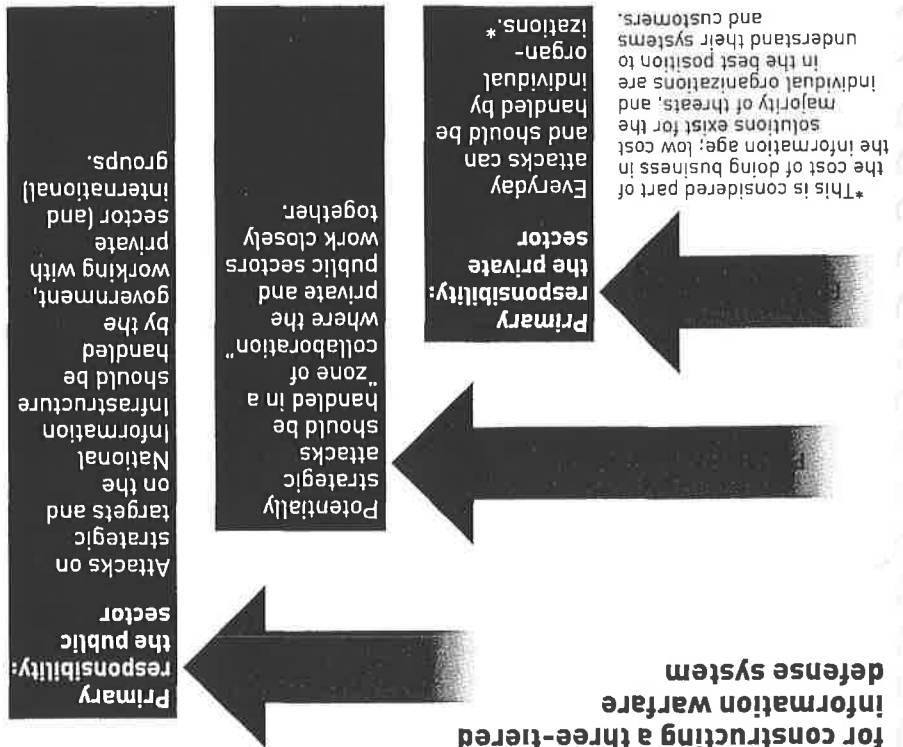
But don't start hoarding food or stuffing money into your mattress just yet. While it's healthy to be aware of what cyberterrorists could do to our electronic or physical infrastructure, both the government and corporate America have a vested interest in keeping records safe and critical systems working. Numerous

Will cyberwarriors become a fifth branch of the military?
 How severely?
 Will it be justified in responding militarily in the real world?

If a government stopped a cyberattack, would it be justified in responding militarily in the real world?
 How severely?
 Will cyberwarriors become a fifth branch of the military?
 Will a computer programmer win the Medal of Honor?

—Paul D. Kretekowski

Division of responsibility for constructing a three-tiered information warfare defense system



DEFENSE IN DEPTH. A comprehensive defense strategy covers three lines of defense — everyday attacks, potentially strategic attacks, and strategic attacks — with responsibility shared between public and private organizations (Albers, Defensive Information Warfare, 1996).

Automatic Face Recognition.. THE ID YOU CAN'T FORGET

WHEN SOME PEOPLE encounter facial recognition technology, they don't like it. "My face is my password? That's too Big Brother for me!" Actually, human beings have used facial recognition as a form of ID for millions of years. But it's only been in the last few years that the technology to determine who you are by your facial features has begun to catch up with our innate ability to differentiate each other at a glance.

Like fingerprints, no two people have the exact facial characteristics. Facial recognition software takes advantage of this by identifying dozens of measurable features, such as the contour of a jaw and chin, the distance between eyes, and the width of a nose. Each of these features is called a *nodal point*. When a digital camera takes a picture of your face, the facial recognition software turns all the nodal points into one long string of numbers, called a *faceprint*. Your faceprint is then compared against all the faceprints in a database to determine who you are. The database might be a "whitelisted" containing faceprints and names of employees who work in a high

Graphic by Bill Smart/Hunter Newsom

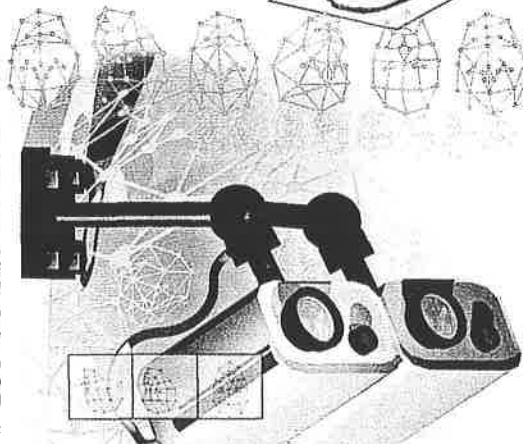
The walls have eyes

Security cameras in stores, banks and even parks may soon start scanning for fugitives. The new Mugsport system uses pattern-recognition software to watch crowds at airports, bus stations and other busy places.

How it works

In about 13 seconds, Mugsport scans a crowd and compares the faces to a database of pictures. Future refinements may cut that time in half. Airports and bus terminals are prime locations, but Mugsport can watch cars at traffic intersections. Computer picks out the heads of people and tracks them, watching for the best view of the subject's face. A geometric grid of 45 points is plotted. Because Mugsport examines facial proportions, hair or disguises won't throw it off. If the computer has only a partial view of the face, it can't plot all 45 points, and the identification is harder.

Three-dimensional facial grids of eight different people



The system creates a keyhole view of each person—sharp and detailed at the center, blurred at the sides. The computer creates an electronic data file called a wavelet transform, then simplifies it into a grid. Modified wavelet. Wavelet. Grid. Software compares each facial grid its database of wanted criminals.

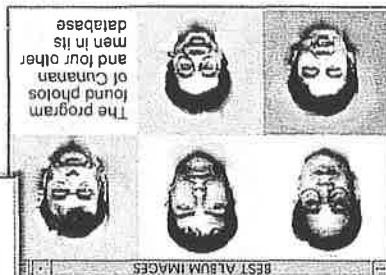


Other ID checking methods

Finger identification: Being tested by MasterCard. When a person opens an account, his or her fingerprint is scanned and a numeric value is loaded onto a card. The holder presses a finger against a small screen, which compares it to the record in the chip.

Hand recognition: The system scans fingers and tops and sides of a hand. It's now in use at San Francisco International Airport, the Colombian legislature and sperm banks, which use it to verify donors.

Face recognition: Software keeps unauthorized people from using a personal computer. A small video camera takes a picture of person, and the computer compares it to images of approved users.



Cunanan test
Researchers had Mugsport scan and analyze a photo of serial killer Andrew Cunanan

It ranked the matches, showing the best one at top left

SOURCES: University of Southern California, Los Angeles; MasterCard; FaceIt; Salk Institute for Biological Studies

BLURRY RESULTS

recognition technology test used to screen employees at the Palm Beach International Airport. The system, called FaceIt, failed to identify the employees 53% of the time. The facial recognition system's manufacturer, Identix, defended itself by saying the system was used with the incorrect lighting and that similar tests in other airports reported only 10% false negatives. FaceIt takes wide photographs of people and converts them into digital fingerprint codes, which are then compared to a database containing fingerprint codes.

wouldn't try to tell who the rider is; it would simply determine the location of a rider's face and aim the air bag to deploy in the proper place on the rider's body. This system would prevent children and small adults from getting injuries from airbags that might otherwise hit them in the face and neck.

PROVOCATIONS...

With automatic facial recognition do you have the right not to be recognized? Will Halloween be the most confusing day of the year?

If you come home with a black eye, will your house let you in?

—Mark Frauenfelder

WANT MORE?

VIISAGE

www.village.com/facialrecog.htm

IDENTIX

www.identix.com

EYEMATIC

www.eyematic.com

ACTU ON FACIAL RECOGNITION

www.actu.org/issues/privacy/

[facial_recognition-faq.html](http://www.facial_recognition-faq.html)

EPIC ON FACIAL RECOGNITION

www.epic.org/privacy/facerecognition

OMRON TECHNOLOGY VENTURES

www.society.oxfordjournals.org

“security building. Or it might be a “black-list” containing the identities of wanted terrorists and criminals. A blacklist of at-large suspects was famously used by Tampa Bay, Florida, police to search for criminals at Super Bowl XXXV, which was dubbed “Snooperbowl” by privacy rights advocates who decry the use of face recognition. The attendees weren’t aware that their faces were being monitored and matched up against a database. At the end of the day, the system succeeded in identifying just 19 petty criminals, such as ticket scalpers and pickpockets.

NICE TO SEE
YOU, TOO!

Researchers at NCR and the USC Integrated Media Systems Center are developing computers that can recognize how you're feeling. A digital camera and specialized software pinpoint facial features and create a map of your emotional state. NCR is interested in applying the technology to ATMs to make them more responsive. Forgot your glasses and can't see the numbers? The computer can detect this and make the type larger. Hate annoying advertisements? Emotion-sensing ATMs could help ease your irritation. But all this begs the question: Do you want a cash machine that can read your mind?

A noncontroversial use for facial recognition technologies is in air bag deployment. A Los Angeles-based company called Eyematic is working with air bag manufacturers to include tiny video cameras and facial recognition technology into their equipment. The software

While facial recognition is an excellent way to prevent unauthorized people from entering a workplace, some security experts have their doubts about its effectiveness as a way to nab criminals at sporting events and terrorists at airports. Bruce Schneier, chief technology officer and Founder of Counterpane Internet Security, Inc., says even a system with a 99.99% accuracy rate will set off 10,000 false alarms for each terrorist it identifies, assuming one in every billion people passing by the video camera is a terrorist. Such a system would create a "boy who cried wolf" scenario," he says, because security personnel would stop taking the alarms seriously. But facial recognition companies argue that the deterrent factor of facial recognition companies is an important feature that isn't taken into account in

