

JANUARY 7, 2003

SPECIAL REPORT: MILITARY TECHNOLOGY

THE STAT

## \$26.4

Global sales of LCD TV sets, in billions, forecast for 2006

[More Vitals On TV Displays >>](#)

BUSINESS DIRECTORY

Find services and products now.

1. Select industry

Technology

2. Select service

- Business Continuity
- Content Management Solutions
- Corporate Training
- CRM Solutions

**FIND**

PREMIUM CONTENT

[MBA Insider](#)

BW MAGAZINE

- [Get Four Free Issues](#)
- [Register](#)
- [Subscribe](#)
- [Customer Service](#)

ONLINE FEATURES

- [Book Reviews](#)
- [BW Video](#)
- [Columnists](#)
- [Interactive Gallery](#)
- [Newsletters](#)
- [Past Covers](#)
- [Philanthropy](#)
- [Podcasts](#)
- [Special Reports](#)

BLOGS

- [Blogspotting](#)
- [Brand New Day](#)
- [Byte of the Apple](#)
- [Deal Flow](#)
- [Economics Unbound](#)
- [Fine On Media](#)
- [Hot Property](#)
- [NussbaumOnDesign](#)
- [Tech Beat](#)

TECHNOLOGY

- [J.D. Power Ratings](#)
- [Product Reviews](#)

## The Network Is the Battlefield

The Pentagon's aim is to meld weapons systems and people into a whole, called network-centric warfare, that's greater than the sum of its parts

On Nov. 21, U.S. Air Force officials got their hands on the ultimate global video game. Thanks to a system upgrade by defense contractor Lockheed Martin ([LMT](#)), flyboys (and girls) could hop onto a special Air Force network from any PC equipped with a Web browser and special military encryption and authentication software. Once on this network, they could call for air strikes, direct reconnaissance planes, or plot the movements of the most powerful flying force on Earth -- all from their laptop in a café (or, more likely, at a secured facility). "All you need is Internet Explorer," says Doug Barton, the director of technology for Lockheed Martin Mission Systems, based in Gaithersburg, Md.

ADVERTISEMENT

This technology has a typically clunky military name -- the TBMCS C2 Air Combat system -- that belies its power. In fact, it isn't a game at all, but the latest in a series of developments that's moving the Air Force into the era of so-called network-centric warfare, or NCW. The goal is to weave weapons systems and people into a network whose whole is far greater than the sum of its parts.

Among other things, the system should make it easier to track and attack military targets, and provide a command structure that's more resilient and damage-proof. "If you network a [military] force, it can do things at a speed that is unimaginable," says John Garstka, an associate director of the Pentagon's Office of Force Transformation and a leading theorist in the area.

**BEST-CASE SCENARIO.** The military's resounding success in Afghanistan, where units from different branches of the service worked in unprecedented unison, has led to a consensus that NCW is the way of the future. "If 20 years ago you had predicted to Army, Navy, and Air Force people the degree to which they would be working together, they would have said no," says Ivan Oelrich, a senior research associate at the Federation of American Scientists. He calls the latest developments "an impressive change in institutional culture."

Now comes the hard part. While the U.S. was able to flatten the Taliban with a minimum of casualties and less damage to civilians than occurred during the Vietnam War, for example, Afghanistan was in many ways a best-case scenario. The Taliban could muster few if any defenses and weren't well trained, equipped, or motivated. And the barren terrain of Afghanistan made communications with satellites and between U.S. units less complex than in a jungle or urban environment.

Even so, many U.S. commanders bumped up against some discouraging limitations of NCW, 2002-style. Stories of Special Forces troopers calling in air strikes with laser pointers made the media, but behind the scenes commanders had to queue up for satellite uplinks and bickering broke out over who would get access to unmanned aerial vehicles (UAVs) with names like Global Hawks or Predators. Many officers complained of bandwidth limitations that crimped their ability to use newly networked systems.

"The further you get out in a deployed scenario, the less bandwidth is available," says Jerry DeMuro, president of the command, control, communication, and computer system (C4)

**STORY TOOLS**

- ▶ [Printer-Friendly Version](#)
- ▶ [E-Mail This Story](#)

**RELATED ITEMS**

- [The Network Is the Battlefield](#)
- [Star Wars by '04? Forget It](#)
- [Tomorrow's Smarter, Connected Navy](#)
- [Adaptive Aircraft: No Flight of Fancy?](#)
- [Playing Defense with Defense Stocks](#)

**TODAY'S MOST POPULAR STORIES**

1. [Fasten Your Seat Belts in '06](#)
2. [TV Madness at CES 2006](#)
3. [The Upstart Buzzing Around El Al](#)
4. [Time Warner: No Disassembly Required](#)
5. [Big Plastic's Online Challenger](#)

[Get Free RSS Feed >>](#)

**MARKET INFO**

DJIA	10714.13	-3.40
S&P 500	1250.53	+2.24
Nasdaq	2204.72	-0.60

**STOCK LOOKUP** **GO**

**Stocks Trade Lower**  
[Create / Check Portfolio](#)  
[Launch Popup Ticker](#)

- Tech Stats
- Wildstrom: Tech Maven
- INNOVATION & DESIGN**
- Home Page
- Architecture
- Brand Equity
- Car Buff
- Game Room
- SMALLBIZ**
- Smart Answers
- Success Stories
- Today's Tip
- Trailblazing Companies
- INVESTING**
- Investing: Europe
- Annual Reports
- BW 50
- S&P Picks & Pans
- Stock Screeners
- Free S&P Stock Report
- SCOREBOARDS**
- Mutual Funds
- Info Tech 100
- S&P 500
- B-SCHOOLS**
- MBA Blogs
- MBA Profiles
- MBA Rankings
- Who's Hiring Grads
- BW EXTRAS**
- BW Digital
- BW Online Alerts
- Dashboard Widgets
- Handheld Edition
- RSS Feeds RSS 2.0
- Podcasts RSS 2.0
- Reprints/Permissions
- Conferences
- Investor Workshops
- Research Services

COLUMNS
FORUMS & CHATS
NEWSLETTERS
PERSONAL FINANCE
SEARCH & BROWSE
SPECIAL REPORTS
TOOLS & SCOREBOARDS
VIDEO VIEWS

- Customer Service
- Contact Us
- Advertising
- Conferences
- Permissions & Reprints
- Marketplace
- Subscribe to BW

unit at defense contractor General Dynamics ([GD](#)). "It's a precious commodity."

**INFORMATION WINS.** Another danger is becoming lulled into thinking that, despite such glitches, the U.S. military is invincible. "How does all this function in the future when we don't have absolute dominance?" wonders the FAS's Oelrich. "That's something the military hasn't thought through at all." Nor has it even contemplated the effort and time required to remake a hierarchial, hidebound organization so that it can function with a flat management structure, ad-hoc collaboration, and on-the-fly decision-making.

Nonetheless, one way or another NCW is coming, for one simple reason: From the dawn of organized conflict, military strategists have used communications and information to beat the enemy. The ancient Greeks dispatched runners over long distances to deliver military messages. European infantries used drummers to communicate common battle orders to solidiers fighting together who didn't speak the same language.

NCW sprang from a need, dramatized in World War II and Vietnam, to use information technology to create a more lethal fighting force, as well as to to avoid casualties from friendly fire. Initial efforts follow what has become a familiar path for new technologies: Each branch of the service went its own way, creating a system that was incompatible with that of the other branches.

**TRIED AND TRUE SYNTAX.** "If I have 14 systems, I have to build 14 interfaces," says Margaret Myers, deputy chief information officer for the Defense Dept. "Then the next guy comes along and builds a new system, and then he or she has to build 15 interfaces. That's expensive, and those interfaces don't always work." The commander of a joint task force comprising sea, air, and land power, and spanning multiple service branches -- the unit used to fight most battles today -- must contend with 400 combat systems, most of which are still incompatible, Myers says.

In the mid 1990s Defense found a solution in the form of the Internet -- a slightly ironic development in that Pentagon research money helped fund the original Internet, ARPANET, which was a small project designed to create easy ways for researchers to communicate electronically that would be hard to disrupt. What Defense wants NCW to use isn't so much the public Internet itself, though a significant percentage of its traffic travels on the Web, but rather the technology behind the Net, the universal syntax called TCP-IP that allows Apple desktops to talk easily with Unix servers, Microsoft-based PCs, and Linux-powered laptops.

Adapting specialized computer battle systems built on proprietary technology to work with standard Internet protocols entails a lot of special programming that, to take one example, ties weapon systems more closely into the global positioning satellite network that provides the coordinates of any location on earth. Add to the mix the growing sophistication and dependability of wireless communications, and the Pentagon not only can guide bombs and missiles with GPS tracking systems but also change their trajectory in mid-flight.

**OVERSOLD ABILITIES?** Suddenly, Navy battle groups of dozens of ships and aircraft can share a radar picture, plus information on everything from incoming low-flying cruise missiles to small boats bearing suicide bombers. The Navy is deploying that capability as part of Raytheon's ([RTN](#)) Cooperative Engagement Capability project, a \$1 billion system that's just now being rolling out.

The progress has been impressive, though observers sound cautionary notes. "The flaw in this is that none of what's being advertised can be done on the stated timelines," says Frank Lanza, CEO of L-3 Communications ([LLL](#)), which builds a wide variety of communication and networking systems for the military. "The danger is that people believe it can be done." Lanza's fear is that a lot of the new NCW equipment and its capabilities are being oversold in their current incarnation.

That may be the case, but the military clearly is tackling some of the more basic problems, such as bandwidth dearth. Sometime in 2004, Defense hopes to conclude a program called Global Information Grid Bandwidth Expansion, or, GIG-BE. The \$500 million project will dramatically increase bandwidth at 90 locations around the world that the U.S. military considers to be critical. The ultimate goal is to create a secure global network with enough capacity to handle real-time image transmission and other capacity-hogging tasks, as well as bringing online many more soliders in battle.

**RISING BURDEN.** Sites that heretofore could transmit data at the rate of 1.5 megabits per second -- the equivalent of a T-1 line that powers a small office building -- will be boosted to 10 gigabits per second, thanks to new terrestrial fiber-optic links owned and operated by commercial companies that contract with the Pentagon.

Just a fraction of the 1.5 million active-duty personnel in the U.S. military now log on to the global network simultaneously -- most of them from bases that remain connected to land-based phone lines. The data burden will surely be considerable when a higher percentage of troops go online, as they inevitably will. "We really don't know how it's going to work until we" try it in a battle situation," says the Pentagon's Gartska. But a thousand-fold increase in capacity can't hurt.

Despite the improvements it will bring, even GIG-BE won't help much with the "last mile" problem -- bringing broadband access to every soldier in the field where they'll most likely be working far from fiber-optic cables common in populated areas of the developed and developing world. In the U.S., that problem is being alleviated on the civilian side to some extent with wireless data hookups -- so-called Wi-Fi 802.11 nodes -- that are sprinkled throughout cities. The military has also adopted secure versions of that technology for stateside communications and for near-shore ship-to-shore data broadcasts.

**NETWORKS ON THE GO.** While the military is also relying on wireless, it faces a far more complex job in making an untethered network function properly. Afghanistan offered no cell towers or Wi-Fi nodes. Network gear of any type has to be flown, floated, or humped in. And once the infrastructure is set up, it doesn't stop moving: It will likely be mounted on vehicles, planes, and ships.

Building software to power and manage such a complex network is tricky, much akin to what Verizon ([VZ](#)) would have to do if cell towers were mounted on trucks, ferries, and taxi-cabs instead of in fixed locations on buildings. "You have mobile infrastructure as well as mobile users," says Jim Quinn, a manager at Lockheed Martin who works on mobile networking for the company's WIN-T (Warfighter Information Network-Tactical) program, a multicompany effort commissioned by the U.S. Army. Mobile everything greatly adds to the complexity of a system, he adds.

The military is working on several ways to tackle the last-mile problem. Using powerful lasers to transmit data from satellites to the ground and from mountain to mountain is one option for extending the broadband pipe. Another is creating technologies that turn every military vehicle into a wireless node, from UAVs to Humvees to helicopters. Such nodes would create a dense mesh that could encompass a battle zone and provide troops with far more reliable connectivity than anything that's available today.

**UNTIMELY CRASHES.** Ultimately, these mesh systems could resemble the peer-to-peer networks that music lovers use to download tunes (most often in violation of copyrights). "We're developing the information grid so that every platform will have the same information, and if one or two platforms fail, their functions are automatically taken over by other platforms. Every platform will be able to be the command center," explains L3's Lanza.

Sounds impressive, except that no one is quite sure how the military will keep such a network from crashing every now and then -- at just the wrong time. "Companies can't keep commercial networks up and running, and we have been in that business for 50 years," says Lanza. For that reason, the services have to engineer such systems with a fall-back option that maintains significant capabilities outside of the network. Lanza explains that the communications systems his company builds for the Global Hawk UAV can be controlled via multiple modes that use UHF, VHF, and other signal ranges.

And to be reliable, these systems can't all operate via the same communications backbone. "You have to be able to create graceful failure modes," says Oelrich. "If everything goes through some central network without which I'm helpless, then what happens if some key node fails?"

**GPS-BLOCKER.** Perhaps the biggest potential problem is that no one thoroughly understands what might happen if a determined enemy attacked these networks. To date, the military has reported that no cyber-attacks, which occur daily, have disrupted operations. "A lot of what

[Defense] is using are dedicated networks. They aren't vulnerable to attack," says Jim Lewis, director of technology policy at the Center for Strategic & International Studies, an influential Washington think tank. "In Kosovo, there were lots of attacks on U.S. computer networks. Not a single sortie [of a U.S. warplane] was stopped."

Though Lewis discounts the danger of hacker attacks, he believes an innovative opponent could throw up countermeasures that might make U.S. military networks far less effective. He points to a device from a Russian company designed to block GPS signals over a radius of thousands of feet. The tiny box sells for several thousand dollars (prices vary depending upon availability) -- but that's still a great deal for any enemy, considering that GPS is a linchpin of NCW strategy.

Worse, Lewis thinks it's possible to make much cheaper versions of the device. Naturally, the military is working on countermeasures to the jamming technology, says L-3's Lanza. But other points of vulnerability exist. The commercial satellite fleet carries a significant amount of military traffic, and "it isn't clear, if we go up against a first-rate opponent, that these satellites will be absolutely secure," says the FAS's Oelrich.

**PASSWORDS IN WRONG HANDS.** In an August, 2002, report, the U.S. General Accounting Office singled out this satellite network as a possible security problem. Indeed, China witnessed the havoc that a technologically determined enemy can wreak when members of the Falun Gong sect commandeered a key Chinese telecommunications satellite in July, 2002, to broadcast so-called propaganda and images of Falun Gong leaders, according to the Chinese government.

Security of the NCW system itself would be an enormous concern. How can Defense be sure that everyone who logs onto the network is who they say they are? Today, if a Special Forces operative is captured with a data device that's logged into the network -- or that has passwords and credentials stored in it -- not much can stop the bad guys from logging on and getting a look at what Uncle Sam is up to. L-3's Lanza says within a few years, continuous biometric authentication will make it harder for unauthorized people to use a stolen machine. For now, though, the problem could be serious, says Defense Deputy CIO Myers.

Using information efficiently will also be a daunting task. The amount of data on the U.S. military's global grid is huge. So how does someone in the field find the right info at the right moment? The solution lies in new network protocols such as XML (extensible markup language), which can tag data with key information that allows software itself to distribute the most relevant information to foxholes.

"One of the biggest challenges will be the greater the connectivity, the more information flows to soldiers. The challenge will be not to overwhelm them," says General Dynamics' DeMuro. That's a vexing problem, though, and one the private sector has yet to solve -- witness the abject failure of most personalization technologies on the Internet. "We will need something like Google on steroids," acknowledges Myers.

**INCOMPLETE VIEW.** Finally, the military will have to deal with the seismic cultural shift that would result from ubiquitous connectivity and data. During the Afghanistan war, a group of top-level commanders was able to watch a UAV lock in on a target via streaming video. Sitting inside the Pentagon, the brass gave the order to fire the missile that destroyed the target -- on the other side of the globe. This capability has a dark side, however. "It's easier for the command to micromanage," says CSIS's Lewis. "There is this impression that instant communications lets us do remote-control war-fighting. And that's a danger."

Why? Often commanders sitting far from the field miss key pieces of local information. And critics call the view from the UAVs, for example, the equivalent of a fish-eye lens on the battlefield.

Perhaps a greater danger could be a temptation for Pentagon mandarins to fall back into old patterns of betting their careers on complex weapons systems. Witness the latest military budget, which contains several big-ticket items, such as the \$200 million-per-plane F-22 fighter. Critics contend that the new jet is more suitable for a Cold War battlefield than for modern conflicts where the difference between a plane that flies at mach 2 vs. mach 1 has little to do with flushing insurgents from jungles or caves.

**INFO INNOVATIONS.** With the federal budget under increasing pressure as the deficit grows and Republicans push for bigger tax cuts, defense insiders fear that the generals may let info-tech upgrades wither at the expense of nifty new toys.


That isn't to say the projects now on the table won't make a big difference. Aside from the Navy's CEC program, the military stands poised to roll out the first so-called tactical radio that connects with legacy radio systems from all three branches. The Pentagon's Garstka believes that the benefits of flattening the military command structure and increasing its networking capabilities will ultimately prove irresistible.

On the battlefield, where improvisation has always been a necessity, GIs and pilots already are using info tech in ways their commanders never imagined -- and sometimes, didn't authorize. Lewis cites instances where forward air controllers and target specialists on bombers have set up instant-message chat sessions to communicate target information in real time using minimal bandwidth. "We're talking about more than just technology," says Garstka. "Wal-Mart and Dell leveraged information technology to change processes and gain competitive advantage. We're trying to do the equivalent in the military."

So it is that in an institution normally immune from change, where decades pass between the initial vision and the implementation of new ideas, Gartska and other gurus of network-centered warfare are making more headway than even they might have dreamed.

---

By [Alex Salkever](#), Technology editor for BusinessWeek Online

Get BusinessWeek directly on your desktop with our [RSS feeds](#). 

Add BusinessWeek news to your Web site with our [headline feed](#).

Click to buy an [e-print or reprint](#) of a *BusinessWeek* or BusinessWeek Online story or video.

To subscribe online to *BusinessWeek* magazine, please [click here](#).

Learn more, go to the [BusinessWeekOnline home page](#)

 [BACK TO TOP](#)