

Index

Cyber Bytes - 10 MAY 11

Articles follow. All articles are accessible via the Internet at the links below.

Links of interest:

CMU Global Connection [research that developed Gigapan]: <http://www.cs.cmu.edu/~globalconn/index.html>

Navy Cyber Command Alignment: RDML Leigher Interview (audio): <http://media.bonnint.net/wtop/21/2155/215586.mp3>

Cyber Risk Analysis: <http://cyberfactors.com/>

The Myth and Reality of Spectrum Scarcity: <http://spectrum.ieee.org/podcast/telecom/wireless/the-myth-and-reality-of-spectrum-scarcity>

Cloud Computing

Agencies to Close 137 Data Centers and Move 100 Email Systems to the Cloud
-<http://www.nextgov.com/nextgov/ng_20110427_1307.php>

Amazon Cloud Failure Takes Down Web Sites
-<<http://bits.blogs.nytimes.com/2011/04/21/amazon-cloud-failure-takes-down-web-sites/>>

Amazon's Trouble Raises Cloud Computing Doubts
-<<http://www.nytimes.com/2011/04/23/technology/23cloud.html>>

Cyber Security

Security Lessons Still Lacking for Computer Science Grads
-<<http://www.infoworld.com/t/application-security/security-lessons-still-lacking-computer-science-grads-769>>

Cyber-Security System Mimics Human Immune Response
-<<http://news.discovery.com/tech/cyber-security-immune-system-110421.html>>

Covert Hard Drive Fragmentation Embeds a Spy's Secrets
-<<http://www.newscientist.com/article/mg21028095.200-covert-hard-drive-fragmentation-embeds-a-spys-secrets.html>>

Index

Cyber Attacks Are Risk of Doing Business (White House)

-<http://www.nextgov.com/nextgov/ng_20110427_6375.php>

Cyber Attacks Rise at Critical Infrastructure Firms

-<http://news.cnet.com/8301-27080_3-20055091-245.html?part=rss&subj=News-Security&tag=feed>

Anonymous to Target Iran With DoS Attack

-<http://news.cnet.com/8301-27080_3-20058700-245.html?part=rss&subj=news&tag=2547-1_3-0-20>

China's Silent Cyber Takeover?

-<<http://the-diplomat.com/flashpoints-blog/2011/04/17/chinas-silent-cyber-takeover/>>

New Password Method Encrypts Like No Other

-<http://www.pcworld.com/businesscenter/article/226099/new_password_method_encrypts_like_no_other.html>

The Botnets That Won't Die

-<<http://www.technologyreview.com/computing/37443/?ref=rss&a=f>>

Meet the Fastest Public-Key Algorithm Few Have Even Heard of

-<<http://www.networkworld.com/news/2011/042011-ntrue-algorithm-x9.html>>

Cyber Identity Strategy Would Eliminate the Need for Multiple Passwords

-<http://www.nextgov.com/nextgov/ng_20110415_8437.php>

Malware and Other Cyber Threats, Many of Which Are State Sponsored, Are Growing

-<http://www.nextgov.com/nextgov/ng_20110420_3403.php>

Cyber War

Is China Winning the Cyber War?

-<<http://fcw.com/articles/2011/04/25/buzz-china-cyber-spying.aspx>>

DOD

Network Would Link Defense Functions, People

Inside the Army's App Store for War

Index

-<<http://www.wired.com/dangerroom/2011/04/armys-app-store-for-war/>>

Pentagon Taps EW for Second Wind

DoD Urged to Rethink Acquisition Managers

Army Enlists Android for Battlefield Comms

-<http://news.cnet.com/8301-13506_3-20056130-17.html?part=rss&subj=News-Wireless&tag=feed>

Navy Cyber Command Alignment: RDML Leigher Interview (audio): <http://media.bonnint.net/wtop/21/2155/215586.mp3>

Five Navy Commands Realigned to Cyber Command in Maryland

ONR's Digital Tutors Give Naval Recruits, High School Students An Academic Edge [video]

-<<http://www.physorg.com/news/2011-04-onr-digital-naval-high-school.html>>

Bin Laden's Computers Will Test US Forensics

-<http://news.cnet.com/8301-31921_3-20060321-281.html?part=rss&subj=news&tag=2547-1_3-0-20>

Information and Society

Iran's Answer to Stuxnet

-<<http://www.technologyreview.com/blog/guest/26692/?ref=rss>>

Federal Radio Navigation Plan Relies on GPS, With No Backup

-<http://www.nextgov.com/nextgov/ng_20110422_3383.php>

Information Technology

Really Remote Data [Data center operations in austere geographies]

-<<http://www.technologyreview.com/computing/37460/?ref=rss&a=f>>

Microsoft Business Suite Wins Federal Certification

-<http://news.cnet.com/8301-10805_3-20055847-75.html?part=rss&subj=news&tag=2547-1_3-0-20>

Carnegie Mellon Researchers Build Time Machine That Allows Visual Exploration of

Index

Space and Time [Gigapan Time Machine]

-<http://www.cmu.edu/news/archive/2011/April/april21_gigapantimemachine.shtml>

A Glimpse Inside One of Google's Data Fortresses [video]

-<<http://newenterprise.allthingsd.com/20110422/a-glimpse-inside-one-of-googles-data-fortresses-video/>>

Chinese Chips Wins Energy Efficiency Crown

-<[http://spectrum.ieee.org/semiconductors/processors/chinese-chip-wins-energyefficiency-crown?](http://spectrum.ieee.org/semiconductors/processors/chinese-chip-wins-energyefficiency-crown?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrum+%28IEEE+Spectrum%29)

[utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrum+%28IEEE+Spectrum%29](http://spectrum.ieee.org/semiconductors/processors/chinese-chip-wins-energyefficiency-crown?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrum+%28IEEE+Spectrum%29)>

Translating the Web While You Learn [CMU]

-<<http://www.technologyreview.com/computing/37487/?ref=rss>>

Targeting Left Over Land Mines

-<<http://news.harvard.edu/gazette/story/2011/05/targeting-leftover-land-mines/>>

Robotics

BAMS Program Office Seeks to Integrate Air Force SIGINT Sensor Into Platform

Do Drones Make War Too Easy?

-<<http://www.dodbuzz.com/2011/04/25/do-drones-make-war-too-easy/>>

X-47B First Flight Hints At New Capabilities For Navy Carriers

Boeing Phantom Ray UCAS Makes First Flight [video]

-<[http://spectrum.ieee.org/automaton/robotics/military-robots/boeing-phantom-ray-ucav-makes-first-flight?](http://spectrum.ieee.org/automaton/robotics/military-robots/boeing-phantom-ray-ucav-makes-first-flight?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrum+%28IEEE+Spectrum%29)

[utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrum+%28IEEE+Spectrum%29](http://spectrum.ieee.org/automaton/robotics/military-robots/boeing-phantom-ray-ucav-makes-first-flight?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrum+%28IEEE+Spectrum%29)>

Future UAVs Must Be Hardened

-<<http://www.defensenews.com/story.php?c=AIR&i=6285209&s=TOP>>

Space

Nearly a Decade Behind Schedule, New Satellite Is to Provide Earlier Missile-launch Warning

Index

-<http://www.nextgov.com/nextgov/ng_20110426_9742.php>

Air Force's First Dedicated SBIRS Satellite Carried to Orbit

-<<http://www.spacenews.com/launch/110509-af-first-sbirs-carried-orbit.html>>

Technology Advances

Top Chinese Supercomputers Point to Aggressive HPC Strategy

-<<http://www.hpcwire.com/hpcwire/2011-04-26/>

[top_chinese_supercomputers_point_the_way_to_aggressive_hpc_strategy.html](http://www.hpcwire.com/hpcwire/2011-04-26/top_chinese_supercomputers_point_the_way_to_aggressive_hpc_strategy.html)>

Intel Increases Transistor Speed by Building Upward

-<<http://www.nytimes.com/2011/05/05/science/05chip.html?partner=rss&emc=rss>>

How Three-Dimensional Transistors Went from Lab to Fab

-<<http://www.technologyreview.com/computing/37536/?ref=rss&a=f>>

Agencies to Close 137 Data Centers and Move 100 Email Systems to the Cloud

Agencies to close 137 data centers and move 100 email systems to the cloud

BY JOSEPH MARKS 04/27/2011

Federal officials on Wednesday released a [list](#) of 137 government data centers slated to close by the end of the year. The information they hold will either be consolidated into other data centers or moved to rented space in a public or private cloud.

Thirty-nine of those data centers already have been shuttered, federal Chief Information Officer Vivek Kundra told a gathering of government and industry officials at a White House event Wednesday.

In addition, 15 federal agencies have identified 100 government email systems comprising nearly 1 million individual email users that will be moved from government-owned data storage space to [cloud computing](#), Kundra said.

The [General Services Administration](#) will begin accepting bids May 10 on a \$2.5 billion contract to manage that move, he said.

Kundra is the author of a December 2010 [plan](#) to fundamentally reform how the government manages information technology projects. That 25-point plan calls for the government to close about 800 of its more than 2,100 data centers nationwide within five years.

Data centers are essentially rooms filled with computer servers that hold government data and operating systems. They can range from just a few rooms to large complexes. Computer clouds are even larger blocks of computers, usually owned by private companies that rent out server space and typically charge customers only for the amount of space they use, which may fluctuate.

The data centers identified for closure collectively take up more than 350,000 square feet and cost the governments tens of millions of dollars annually in upkeep, staffing and electricity, Kundra said.

"Imagine five-and-a-half football fields filled with servers and networks and routers and switches, consuming energy and requiring cooling," Kundra said, "and it poses a huge [cybersecurity](#) threat."

The Health and Human Services Department was spending \$1.2 million annually for electricity at one data center in Rockville, Md., that has since closed, Kundra said.

An internal audit showed many federal data centers were underutilized and operated with little oversight. It took several months simply to determine how many federal data centers even existed.

Agencies to Close 137 Data Centers and Move 100 Email Systems to the Cloud

Kundra said Wednesday that the government was using only about 40 percent of the available space in existing data centers and that, on average, data center servers were operating at about 27 percent of their capacity.

The government plans to create an internal marketplace for storage space in the remaining federal data centers so they'll all be operating close to capacity. Other data currently in federal data centers will be moved to the cloud.

The Defense Department is, by far, the largest current owner of federal data centers, with more than 750 of the roughly 2,100 total. Of the 137 data centers planned for closure by 2012, 57, or nearly half, belong to Defense.

Of the 39 centers already closed, NASA owned 13 while Defense owned eight and the Commerce Department owned six. Other data centers were owned by the Interior, State, Transportation and Homeland Security departments, among others.

Kundra noted that closing data centers will become more difficult now that the list of centers is out and the closures can be linked to jobs in particular congressional districts.

In response to an audience question, Kundra downplayed concerns about the security of storing federal data in privately owned clouds, noting that more than 4,700 government technology systems already are being operated by highly certified government contractors.

"For some weird reason, the risks are being overly-hyped," Kundra said. "When you look at cloud computing, you need to make sure on a case-by-case basis, you're evaluating the risks as in any other platform ... Agencies are being very mindful that they're moving to the cloud in a very safe, secure manner rather than just moving haphazardly in that direction."

A private cloud owned by Amazon crashed temporarily last week, taking with it a minor Energy Department website dedicated to sharing clean energy tips. Other federal sites on the Amazon cloud were unaffected.

Amazon Cloud Failure Takes Down Web Sites

April 21, 2011, 4:40 PM

Amazon Cloud Failure Takes Down Web Sites

By [CLAIRE CAIN MILLER](#)

10:28 a.m. | **Updated** *to reflect status of the problem on Friday.*

A widespread failure in Amazon.com's Web services business was still affecting many Internet sites [on Friday morning](#), highlighting the risks involved when companies rely on so-called cloud computing.

The problems, which began early Thursday morning, affected sites including Quora.com, Reddit.com, GroupMe.com and Scvngr.com, which all posted messages to their visitors about the issue. Most of the sites have been inaccessible for hours, and others were only partly operational.

The Web companies use Amazon's cloud-based service to serve their Web sites, applications and files. Amazon's customers include start-ups like the social networking site Foursquare but also big companies like Pfizer and Nasdaq.

Amazon, which is a leader in this business, lets these companies rent space on its servers and take advantage of its big data centers and computing power. But that gives the companies little control if the servers fail.

"We don't think the cloud is enterprise-ready," said Jimmy Tam, general manager of Peer Software, which provides data backup for businesses. "Are you really going to trust your corporate jewels to these cloud providers?"

Executives at the Web companies that are Amazon customers said that while they knew of the risk, the failure was still frustrating. They said they were investigating options to avoid similar problems in the future.

"Clearly you're not in control of your data, your information," said Campbell McKellar, founder of Loosecubes, a Web site for finding temporary workspace that was not

Amazon Cloud Failure Takes Down Web Sites

available Thursday. “It’s a major business interruption. I’m getting business interruption insurance tomorrow, believe me, and maybe we get a different cloud provider as a backup.”

Other Web companies said cloud computing was a necessity.

“The benefits of the cloud are significant,” said Jeff Janer, chief executive of Springpad, a service that people use to save items online, which went offline as a result of Amazon’s problem. “Amazon as a resource for a company like ours makes an awful lot of sense. We’re just all keeping our fingers crossed that they get back as quickly as possible.”

The problems also affected some functions of the Web site of The New York Times, including the ability to comment on articles.

Amazon did not respond to requests for comment. The company was updating the status of its Web services online and confirmed disruptions at a data center in Northern Virginia. The page said it was unknown when the services would be restored.

Amazon's Trouble Raises Cloud Computing Doubts

April 22, 2011

Amazon's Trouble Raises Cloud Computing Doubts

By **STEVE LOHR**

As technical problems interrupted computer services provided by [Amazon](#) for a second day on Friday, industry analysts said the troubles would prompt many companies to reconsider relying on remote computers beyond their control.

“This is a wake-up call for cloud computing,” said Matthew Eastwood, an analyst for the research firm IDC, using the term for accessing services and information in big data centers remotely over the Internet from anywhere, as if the services were in a cloud. “It will force a conversation in the industry.”

That discussion, he said, will most likely center on what data and computer operations to send off to the cloud and what to keep inside the corporate walls.

But another issue, Mr. Eastwood said, will be a re-examination of the contracts that cover cloud services — how much to pay for backup and recovery services, including paying extra for data centers in different locations. That is because the companies that were apparently hit hardest by the Amazon interruption were start-ups that, analysts said, are focused on moving fast in pursuit of growth, and less apt to pay for extensive backup and recovery services.

Amazon set up a side business five years ago offering computing resources to businesses from its network of sophisticated data centers. Today, the company is the early leader in the fast-growing business of cloud computing.

Amazon's Trouble Raises Cloud Computing Doubts

In business, the cloud model is rapidly gaining popularity as a way for companies to outsource computing chores to avoid the costs and headaches of running their own data centers — simply tap in, over the Web, to computer processing and storage without owning the machines or operating software.

Amazon has thousands of corporate customers, from [Pfizer](#) and [Netflix](#) to legions of start-ups, whose businesses often live on Amazon Web Services. Those reporting service troubles included Foursquare, a location-based social networking site; Quora, a question-and-answer service; Reddit, a news-sharing site; and BigDoor, which makes game tools for Web publishers.

The problems companies reported varied, but included being unable to access data, service interruptions and sites being shut down.

Amazon has data centers around the world, but the current problems have come from its big center in Northern Virginia, near Dulles airport. Amazon's Web page on [the status of its cloud services](#) said on Friday that matters were improving but were still not resolved. A company spokeswoman said the updates would be Amazon's only comment for now.

Big companies, that have decided to put crucial operations on Amazon computers are apt to pay up for the equivalent of computing insurance, analysts say. Netflix, the movie rental site, has become a large customer of the Amazon cloud. Most of its Web technology — customer movie queues, search tools and the like — runs in Amazon data centers.

Netflix said it had sailed through the last couple of days unscathed. "That's because Netflix has taken full advantage of Amazon Web Services' redundant cloud architecture,"

Amazon's Trouble Raises Cloud Computing Doubts

which insures against technical malfunctions in any one location, said Steve Swasey, a Netflix spokesman.

BigDoor, a 20-employee start-up in Seattle, was knocked down by Amazon's travails. It had backup and recovery services with Amazon, said Keith Smith, the chief executive, but only at Amazon's data center in Virginia. "There's always a trade-off," Mr. Smith said, noting the expenses and developer time that would have been required to do more.

By Friday evening, most services at BigDoor, which makes game and rewards features for online publishers, were back up, but its Web site was still down.

The long-term toll to cloud computing, if any, is uncertain. Corporate cloud computing is expected to grow rapidly, by more than 25 percent a year, to \$55.5 billion by 2014, IDC estimates.

Major technology suppliers are aggressively promoting different cloud offerings — some emphasizing a utility-style service, like Amazon, and others focusing more on selling big companies the hardware and software to more efficiently juggle computing workloads. The latter use the cloud technology, but companies own and control them — so-called private clouds.

The Amazon interruption, said Lew Moorman, chief strategy officer of Rackspace, a specialist in data center services, was the computing equivalent of an airplane crash. It is a major episode with widespread damage. But airline travel, he noted, is still safer than traveling in a car — analogous to cloud computing being safer than data centers run by individual companies.

Amazon's Trouble Raises Cloud Computing Doubts

“Every day, inside companies all over the world, there are technology outages,” Mr. Moorman said. “Each episode is smaller, but they add up to far more lost time, money and business.”

The Amazon setback, he said, should prove to be a learning experience. “We all have an interest in Amazon handling this well,” said Mr. Moorman, whose company is a competitor in the cloud business.

Security Lessons Still Lacking for Computer Science Grads

Security lessons still lacking for computer science grads

Computer science majors have good job prospects, but the vast majority lack an understanding of security and the fundamentals of secure programming

By Robert Lemos | InfoWorld



This year's crop of college graduates are preparing to leave school and join the workforce, and the computer science majors among them appear to have good prospects. Development and software engineering jobs have grown significantly over the last five years, [according to job site Indeed.com](#), with software engineers for social media, mobile applications, and cloud infrastructure currently in the highest demand. In fact, the U.S. Bureau of Labor Statistics expects jobs for software engineers -- who design applications -- to [grow by a third](#) in the next seven years.

Yet in one key way today's graduates are unprepared to enter the workforce: The vast majority will lack a solid understanding of computer security and how to make their applications secure, experts say. Most top computer science programs don't require students to learn the fundamentals of secure programming -- an oversight that will continue to hurt application security in

Security Lessons Still Lacking for Computer Science Grads

the future, said David Koretz, CEO of security firm Mykonos Software.

"If you look at computer science and software engineering programs today ... the crazy thing that blew me away is there is not a single required class on security for any of our computing science or software engineering grads," Koretz said. "You can go through five years of training and yet you will not know anything about security."

This week Mykonos became the latest company to start working with undergraduate programs -- in this case the Rochester Institute of Technology in New York -- to improve the security preparedness of computer science graduates. Microsoft also has made calls for better training of graduates and worked with undergraduate programs to add security education to their curriculum. And last year [Solera Networks offered universities a free security appliance](#) if they used it in their training.

In 2009, the Center for Strategic and International Studies, the SANS Institute, and the U.S. Department of Defense (DoD) [launched a series of contests](#) aimed at training students and workers in computer security. Known as the [U.S. Cyber Challenge](#), the program hopes to make up an [estimated shortfall of 10,000 security professionals](#).

Getting security into computer science curricula is a necessary step in helping software developers prevent the thousands of vulnerabilities discovered every year in applications. High-profile breaches of major online service providers -- such as Google, Twitter, and marketer [Epsilon](#) -- have highlighted the need for more secure programming.

"To me, not only is it not surprising [that we are seeing these incidents], it seems exactly what we set ourselves up for," Koretz said.

This article, "[Security lessons still lacking for computer science grads](#)," was originally published at [InfoWorld.com](#).

Security Lessons Still Lacking for Computer Science Grads

Cyber-Security System Mimics Human Immune Response

CYBER-SECURITY SYSTEM MIMICS HUMAN IMMUNE RESPONSE

In the future, a computer virus may be wiped out in much the same fashion that humans overcome a cold.

By [Eric Niiler](#)

Thu Apr 21, 2011 01:35 PM ET

THE GIST

- **Cyber-security experts hope that computers in the future will be able to monitor their own health just like the cells inside our bodies.**
- **The security system could include a "healthy ecosystem" of computers that collaborate to fight threats.**
- **This technology would help computers overcome an ever-increasing number of digital security challenges.**

Computer scientists and IT engineers are increasingly looking to the human immune system as a model for preventing attacks by cyber-hackers. They hope that in the near future computers will be able to communicate among themselves, recognize threats, and be able to monitor their own health -- just like the cells inside our bodies.

"We want the machines to take a more active part in their own protection," said Bruce McConnell, senior counselor for cyber security at the U.S. Department of Homeland Security. "We want to use their brains to protect themselves, but always in the context of the policies of the system administrators and owners."

McConnell is co-author of a new DHS white paper, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action."

No, it's not the dawn of Skynet. But it may be a new way of looking at how computers can be protected, and at the broader questions of privacy versus security. McConnell and others point to a marked increase in cyber-threats from organized crime, terrorists, and nation-states looking for key military, financial and other classified intelligence.

The paper imagines a "healthy ecosystem" of computers that collaborate to fight threats, adapt rapidly, and identify and defeat problems. Right now, computers are not very good at catching things that they haven't seen before, McConnell said. In contrast,

Cyber-Security System Mimics Human Immune Response

the human immune system has evolved to fight intruders that it doesn't recognize. "It says: "This is not me. Maybe I need to send something down there to take a look at it, and maybe quarantine it." McConnell said.

McConnell says a first step would be to get computers to recognize and react to threats automatically. "Right now it's manual," he said, meaning that a human manager has to contact another human manager via e-mail to warn of a virus or other threat. Ideally, that notification would be done instantly between machines at different government agencies.

Some experts are already working on this kind of interoperability on a small scale. One of the biggest obstacles in getting computers closer to working by themselves is figuring out a better way to authenticate interactions, according to Hart Rossman, vice president for cyber-security services at Science Applications International Corp (SAIC).

"Computers are limited by their programming," Rossman said. "If it doesn't model the known versus the unknown, they can't tell the self from the other."

Rossman says experts are looking at new models of "nature-inspired defense" as computer threats become a greater security problem for government agencies and a bigger cost to industry.

"The threat is growing," Rossman said. "There are more incidents and they are becoming more sophisticated. The latest buzzword is 'advanced persistent threats.' These are sufficiently advanced methods that are difficult to detect and take a long time to discern."

Rossman said the DHS paper is a positive response to threats that are on the rise, and is provoking discussion among cyber-security experts.

Another hurdle faced by computer experts in designing collaborative systems of either individual devices or networked computers is that of privacy. How much information should be shared in the name of security?

Angelos Stavros is a computer scientist at George Mason University. He says the more that computers share information in order to deter threats, the more individual privacy is reduced.

Cyber-Security System Mimics Human Immune Response

"Although we want the cell to be curable, we want it to have our private personality that cannot be wiped or automatically checked," Stavros said. "What is an attack? It is often in the eye of the beholder."

Covert Hard Drive Fragmentation Embeds a Spy's Secrets

Covert hard drive fragmentation embeds a spy's secrets

21 April 2011 by [Paul Marks](#)

GOOD news for spies. There is now a way to hide data on a hard drive without using encryption. Instead of using a cipher to scramble text, the method involves manipulating the location of data fragments.

The inventors say their method makes it possible to encode a 20-megabyte message on a 160-gigabyte portable hard drive. It hides data so well that its existence would be "unreasonably complex" to detect, they say.

Encryption should sometimes be avoided, says Hassan Khan at the University of Southern California in Los Angeles, because the gobbledegook it creates is a dead giveaway: it shows someone might have something to hide. That could spell disaster for someone trying to smuggle information out of a repressive country.

So "[steganography](#)", hiding data in plain sight, is coming to the fore. Normally, data intended to be secret is added to the pixels in digital images, or used to change the transmission timing of internet packets. But these techniques are well known and easily detected, says Khan. So, with colleagues at the National University of Science and Technology in Islamabad, Pakistan, he has developed an alternative.

Their technique exploits the way hard drives store file data in numerous small chunks, called clusters. The operating system stores these clusters all over the disc, wherever there is free space between fragments of other files.

Khan and his colleagues have written software that ensures clusters of a file, rather than being positioned at the whim of the disc drive controller chip, as is usually the case, are positioned according to a code. All the

Covert Hard Drive Fragmentation Embeds a Spy's Secrets

person at the other end needs to know is which file's cluster positions have been encoded.

The code depends on whether sequential clusters in a file are situated adjacent to each other on the hard disc or not. If they are adjacent, this corresponds to a binary 1 in the secret message. If sequential clusters are stored in different places on the disc, this encodes a binary 0 (*Computers and Security*, DOI: [10.1016/j.cose.2010.10.005](https://doi.org/10.1016/j.cose.2010.10.005)). The recipient then uses the same software to tell them the file's cluster positions, and hence the message. The researchers intend to make their software open source.

"An investigator can't tell the cluster fragmentation pattern is intentional- it looks like what you'd get after addition and deletion of files over time," says Khan. Tests show the technique works, as long as none of the files on the hard disc are modified before handover.

"The real strength of this technique is that even a completely full drive can still have secret data added to it – simply by rearranging the clusters," adds Khan.

Others are impressed with the technique but see limitations.

"This type of steganography could be used by spies, police or informants - but the risk is that it requires direct contact to physically exchange the USB device containing the secret data," says Wojciech Mazurcyk, a steganographer at Warsaw University of Technology in Poland. "So it lacks the flexibility of internet steganography. Once you embed the secret data on the disk it is not easy to modify it."

But won't making the covert hard disk software open source – as the group plans - encourage its use by criminals and terror groups?

"It's how security vulnerability disclosure works," says Khan. "We have

Covert Hard Drive Fragmentation Embeds a Spy's Secrets

identified that this is possible. Now security agencies can devise techniques to detect it." He adds that his team have had no issues with either US or Pakistani security agencies over their development of this secret medium - despite current political tensions between the two nations.

"The use of steganographic techniques like this is likely to increase," says Fred Piper, director of information security at Royal Holloway, University of London. "Eavesdroppers can learn much from the fact that somebody is encrypting a message."

Cyber Attacks Are Risk of Doing Business

White House official: Cyber attacks are risk of doing business

BY JOSH SMITH, NATIONAL JOURNAL 04/27/2011

The White House official tasked with coordinating the country's response to cyber threats said Wednesday that the risk of such attacks is often overblown.

Howard Schmidt, the White House cybersecurity coordinator, told *National Journal* that a few sensational events make the overall cyber threat seem worse than it really is.

"It's still a situation where specific incidents make it something it's not," he said. "Things make headlines that are just the risk of doing business in many cases."

On Tuesday, Sony announced that hackers stole reams of personal information on 77 million Playstation Network accounts. Last month the Epsilon marketing company lost information on 250 million people to a cyber attack.

But, Schmidt said, compared to other, more traditional crimes, attacks in cyberspace remain rare. He said there had been some successes, although he gave no details.

That being said, Schmidt added, the relatively low risk doesn't mean the problem should be ignored.

Despite concerns by some analysts that the White House cybersecurity office lacks the authority or resources needed to do the job, Schmidt said he has been given everything he needs and is meeting provisions in the Cyberspace Policy Review, among other goals.

While "the government has to do what it can to secure our own systems," Schmidt said, the broader effort to secure networks and information must be managed by both the government and industry.

"It's all government, all private sector," he said. "It's what we refer to as a shared responsibility."

Cyber Attacks Rise at Critical Infrastructure Firms

APRIL 18, 2011 5:13 PM PDT

Cyber attacks rise at critical infrastructure firms

by [Elinor Mills](#)

Cyber attacks on critical infrastructure companies are on the rise, with a jump in extortion attempts and malware designed to sabotage systems, like Stuxnet, according to a new report.

While attacks are increasing, many companies aren't doing enough to protect their systems and are instead rushing to adopt new technologies--such as Smart Grid--without ensuring they adequately secure against cyber attacks, concludes "In the Dark: Crucial Industries Confront Cyberattacks."

The report, due to be released on Tuesday, was commissioned by McAfee and written by the [Center for Strategic and International Studies](#) (CSIS). It includes results from an electronic survey of 200 IT security executives from firms that provide oil, gas, electricity, water, and sewage services in 14 countries during the last quarter of 2010.

Security at power companies has been a concern for decades, but the issue rose to prominence with the emergence last year of the Stuxnet malware, which exploits holes in Windows systems and targets a specific Siemens SCADA (supervisory control and data acquisition) program with sabotage. After dissecting the malware, [experts say](#) they believe it was written to target nuclear facilities in Iran.

"Stuxnet changed the game in our awareness," Phyllis Schneck, vice president and chief technology officer for public sector at McAfee, said in an interview. "Attacks are being developed directly for the capability of creating events on a physical infrastructure."

About 70 percent of the survey respondents said they frequently found malware designed to sabotage their systems during 2010, and nearly half of those in the electric industry said they found Stuxnet on their systems. It was unknown if any of the systems were impacted as a result of Stuxnet, but close to 60 percent said their firms had launched special security audits because of the malware.

The threat from sabotage includes electrical smart grids, which are being quickly adopted without adequate security measures in place, [according to](#) the U.S. Government Accountability Office and

Cyber Attacks Rise at Critical Infrastructure Firms

independent security experts. Fifty-six percent of the respondents whose companies are planning new smart grid systems also plan to connect to the consumer over the Internet. But only two-thirds have adopted special security measures for the smart grid controls, the report said.

"We could end up with a grid connected to peoples' homes that is not properly secured from a cyber attack," said Schneck. "If that system could be turned against itself, that is a disaster waiting to happen."

Another trend happening with critical infrastructure companies is extortion. One in four survey respondents said they had been victims of extortion through cyber attacks or threats of attack with the number of companies subject to extortion increasing by 25 percent over last year. India and Mexico had particularly high rates of extortion attempts, the report found.

"That could be an attempt to crash the network or it could be a denial-of-service attack," or threats to collapse the power grid, said Stewart Baker, a fellow at the CSIS.

Modest security improvements

In general, the report showed increasing levels of attacks and concern about attacks, but modest improvement in security. About 40 percent of the respondents said they believed that their industry's vulnerability had increased and nearly 30 percent said they did not think their company was prepared for a cyber attack.

"More than 40 percent of the executives we interviewed expect a major cyberattack within 12 months--an attack, that is, that causes severe loss of services for at least 24 hours, a loss of life or personal injury, or the failure of a company," the report said. That worry was most intense among executives from India, Mexico, and China.

Things have changed significantly from even one year ago. In 2009, nearly half of the respondents said they had never faced network intrusions or large-scale denial-of-service (DoS) attacks. Now, about 80 percent of respondents said their firms had been targeted by at least one big DoS attack and 85 percent had seen network intrusions. One-quarter reported daily or weekly DoS attacks and one-quarter said they had been victims of extortion through network attacks or the threat of such

Cyber Attacks Rise at Critical Infrastructure Firms

attacks.

Despite the increase in threats and the executives' concerns about them, companies aren't beefing up their security much. Energy firms, for instance, increased their adoption of security technologies by only a single percentage point, to 51 percent, and oil and gas companies by three percentage points, to 48 percent. Brazil, France, and Mexico are lagging in their security responses, adopting only half as many security measures as the leaders in security--China, Italy, and Japan, according to the report.

China and Japan, which both report high levels of formal and informal interaction with their government on security topics, are among the countries with the highest confidence levels that laws will prevent or deter attacks in their countries. Meanwhile, respondents in the U.S., Spain, and U.K. reported little to no contact with their government on security. While all of the Japanese respondents' firms had been audited by their government for security, only 6 percent of those in the U.K. had been.

Companies seem to have a relatively high degree of mistrust for foreign countries. About 60 percent blame nation states and other governments for being behind attacks. The United States was named as the country of most concern for 2009, followed by China, the country called out in the attacks on Google **last year**. China took the top spot last year, according to the survey, which was conducted before reports began surfacing late last year that linked the U.S. to Stuxnet.

Speculation that the U.S. was behind Stuxnet, with some help from Israel, is backed by reports in The New York Times, including **one that says** Siemens gave U.S. researchers the opportunity to identify holes in its software.

Summing up the report's conclusions, Baker of the CSIS said he was worried that the people tasked with making sure we have gas, water, and electricity in our homes and offices aren't doing enough to protect that critical infrastructure.

"The message is that our industrial control systems are very, very vulnerable to attack and the security we have installed today is insufficient to protect us," he said. "I'm concerned that (the

Cyber Attacks Rise at Critical Infrastructure Firms

industry) is not getting that message, despite having the evidence in front of us."

Anonymous to Target Iran With DoS Attack

April 29, 2011 6:47 PM PDT

Anonymous to target Iran with DoS attack

by Elinor Mills



Anonymous says its next target is Iran.

The hacker group Anonymous has its next denial-of-service (DoS) target in sight: Iran, CNET has learned.

Members of the loosely organized group are planning "Operation Iran," an attack designed to shut down Iranian Web sites beginning Sunday, according to their latest [online proclamation](#). May 1 is International Worker's Day.

"The people of Iran have the admiration of Anonymous, and the entire world," the statement says.

"We can see that Iran still suffers at the hands of those in power. Your former government has seized control, and tries to silence you. People of Iran--your rights belong to you."

The operation seemed to already have begun late today with Web page defacements ostensibly targeted at Iranian hackers. Anonymous left messages on several Web sites that had allegedly been previously attacked by the Iranian Cyber Army, including [the site](#) of a Canadian information systems firm and the site of a [Ukrainian dancing group](#), according to an observer on an Anonymous Internet Relay Chat channel that members use to coordinate their operations.

Anonymous is known for its renegade cyberattacks in defense of perceived underdogs or to support freedom of expression or other anti-establishment causes. In defense of whistle-blowing site WikiLeaks, the group targeted PayPal, Visa, MasterCard, and other companies [late last year](#) that had stopped enabling WikiLeaks to receive contributions.

Earlier this month, Anonymous [targeted Sony](#) in protest of the company's treatment of [Sony PlayStation](#) hacker George Hotz. Hotz and Sony have since settled the lawsuit Sony filed, and Anonymous has denied any involvement in a [recent serious breach](#) that exposed information of millions of Sony PlayStation Network customers.

Other Anonymous targets have been: [Broadcast Music Inc.](#), the Church of Scientology; the governments of Egypt, Iran, and Sweden; the Westboro Baptist Church; conservative activist billionaires Charles and David Koch and [their companies](#); as well as security firm HBGary Federal, which had reportedly been working with the FBI to identify the leaders of Anonymous.

China's Silent Cyber Takeover?

China's Silent Cyber Takeover?

By Jeffrey Carr

April 17, 2011

According to the Go proverb 'Play on the Point of Symmetry,' when right and left have the same shape, there's play in the centre. The ancient Chinese game of Go provides an apt metaphor for how China and Russia are leveraging US multinational corporations' economic requirements to accomplish strategic goals that could quite plausibly include covert technology transfer of intellectual property, access to source code for use in malware creation and backdoor access to critical infrastructure.

Take the case of Chinese entity Huawei Symantec. Although Huawei has reportedly been blocked by the Committee on Foreign Investment in the United States (CFIUS) in its effort to acquire 3Leaf, and AT&T was said to be officially discouraged from purchasing equipment from Huawei by the National Security Agency (both due to national security concerns), Huawei successfully formed a joint venture with Symantec in 2007 called Huawei Symantec Technologies Co. Ltd. (HS). Huawei is the majority partner with 51 percent ownership, with the entity being headquartered in Chengdu, China.

According to the Huawei Symantec website:

'Huawei Symantec Technologies Co. Ltd. (Huawei Symantec) is a leading provider of network security and storage appliance solutions to enterprise customers worldwide. Our solutions are developed to keep pace with evolving risks and demanding availability requirements facing enterprises. As a joint venture, Huawei Symantec combines Huawei's expertise in telecom network infrastructure and Symantec's leadership in security and storage software to provide world-class solutions that address the ever-changing needs in network security and storage for enterprises.'

However, a 2008 corporate briefing describes the history, capabilities, and business goals of HS, one of which is to 'build China's first laboratory of attack and defense for

China's Silent Cyber Takeover?

networks and applications.’

Following all this to its logical conclusion, this essentially means that Symantec, a major US information security company, is ‘assisting’ China’s cyber security research in computer network attack and defence -- research that has high potential for abuse by state and non-state actors in China.

In the last few months, HS has formed two new joint ventures with US companies -- SYNEX and Force10 Networks. Why? In the case of SYNEX, the goal is apparently to ‘distribute Huawei Symantec’s storage and security products to its resellers throughout North America.’

For Force10 Networks, Huawei Symantec said the firm ‘is pleased to establish this strategic partnership with Force10 Networks, and expects the relationship to further drive strong results for our existing North American customer base as well as tap into new business opportunities.’

Both SYNEX and Force10 Networks currently sell to the US government. Force10 Networks’ [website](#) says that they sell their products to ‘defense, intelligence and civilian agencies to advance the bandwidth needs and reliability demands of government IT infrastructure while ensuring the economics and performance of mission critical networks.’ Since Huawei’s growth strategy includes financial support from Chinese banks that enable it to offer very low cost bids on key contracts, and since many governments (including India and the United States) have legal provisions that require them to go with the lowest bidder, these partnerships provide an apparently winning strategy for SYNEX and Force10 Networks to secure government sales thanks to Huawei Symantec’s low manufacturing costs - all without HS’s name likely ever having to appear on the contract.

This means that Huawei, while being publicly blocked by US lawmakers from selling directly to the US government, has played on the ‘point of symmetry’ and has quietly secured access to US Defence Department and intelligence community customers through collaborative partnerships that no one has so far contested.

China's Silent Cyber Takeover?

It's not just China that seems to be placing itself in an advantageous strategic position.

Intel's work in the Russian Federation dates back to 2002 with its sponsorship of a laboratory on wireless technology at Nizhny Novgorod State University (NNGU). The laboratory, located in the Department of Radiophysics, benefits from NNGU's decades-long experience with Russia's defence industry, especially the radar and air defence sector. According to an August 2004 *Businessweek* [article](#), the lab was working on security software for high-speed wireless applications.

The laboratory's activity is overseen by a guidance board that includes Leonid Yurevich Rotkov, the head of the [Center for Security of Information Systems and Telecommunications Facilities](#) also located in NNGU's Department of Radiophysics. Leonid Rotkov is a noted expert on IT security. Conference agendas show he works as a security consultant for the Federal Security Service (FSB).

Until around 2008, the Center's website stated that it was sponsored by the Federal Security Service (FSB). This statement has since been removed. However, the faculty listing for the Center includes one individual who is also an employee of the Nizhny Novgorod Branch of Scientific Technical Center (STC) Atlas. STC Atlas was previously directly subordinate to the FSB, however, it's now a Federal State Unitary Enterprise (government owned) research institute that still works on IT security. The Nizhny Novgorod branch is one of four major STC Atlas research facilities. STC Atlas is currently certified by FSB for work on security issues including cryptology and 'special studies.'

The physical location of Intel's lab in a building that seems to be controlled by the FSB; performing research in a key area of interest to the FSB; and if the web evidence is to be believed is overseen by a person who worked as a security consultant for the FSB, could all potentially pose a significant security conflict for Intel's US government customers, one that has been made even more complex by Intel's recent acquisition of McAfee and its announced interest in acquiring database security firm Sentrigo. This is especially so as cloud services are one of Russia's top R&D investment priorities according to the Russian Academy of Sciences.

Additional leverage is afforded to the Russian government through article 15 of Federal

China's Silent Cyber Takeover?

law N 40-FZ 'On the Federal Security Service.'

This is a substantial threat vector because it seems to legally enable the FSB to view or ask for modifications in whatever proprietary data it wants from Intel Russia. In the past, this type of information access would have to be done through espionage. Now it can be done with a simple request. Considering Intel's recent announcement that it's working on a chip-based solution to end the zero-day malware problem, the FSB's access to Intel's technology could make any present or future solution by the company questionable, at best.

So, should US firms shun Russia and China? The economics of continued growth for many US multi-national corporations means that they can't afford to turn away from conducting business in Russia or China. This necessity, when combined with the inherent security weaknesses of a networked world, could be leveraged by the governments of Russia and China to advance their political goals against the United States and other nation states without having to resort to traditional warfare.

This strategy is perfectly legal and can be implemented with complete plausible deniability. Yet almost no one outside of the US national security community appears ready to offer a counter-strategy.

Jeffrey Carr is an IT security analyst and the author of 'Inside Cyber Warfare: Mapping the Cyber Underworld'

New Password Method Encrypts Like No Other

Apr 27, 2011 1:26 am

New Password Method Encrypts Like No Other

By James Mulroy, PCWorld

Have you had an account hacked, or had your personal information stolen? Do you have data that needs to be protected? Fear no more. Researchers from the [Max-Planck-Institut fur Physik komplexer Systeme](#) and from [Axioma Research](#) have devised a new method to create passwords that are harder to hack, but easier to remember.

faboo Comments

Now how did they do that? The researchers combined what's called "nonlinear dynamics" and chaos to create encrypted p-CAPTCHAs (the 'p' stands for password). Sounds complex on the surface, doesn't it? What's even more fascinating is that all you would have to remember is part of the password, and a Java applet will remember the rest for you.

So let's say that you have an important application for a defense contractor that you need to protect and encrypt. Using the Java applet, you would first break your password down into two parts--the easy part and the complex part. You would jot down the easy part of the password and then the java applet would create a [CAPTCHA](#) of the hard part. Then p-CAPTCHA would then be encrypted, using the easy part. When you want to get to your application, you would simply enter the easy part of the password; the p-CAPTCHA would appear, and from there you would interpret it and enter what the image says, thus completely decrypting your file.

According to the paper "[The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs](#)" the second component of the password is "transformed into a CAPTCHA image and then protected using evolution of a two-dimensional dynamical system close to a phase transition, in such a way that standard brute-force attacks

New Password Method Encrypts Like No Other

become ineffective." Not only are brute-force approaches ineffective now, but the researchers say that combined with an [AES](#) algorithm, "a brute-force attack is infeasible both presently and, probably, in the future."

When you create the "easy" part of the password, you can still make it as difficult to guess as you did before, if not more difficult. But when--or *if*--the attacker manages to get the p-CAPTCHA to be generated by the Java applet it will require human interpretation. When you first create the password, the p-CAPTCHA is generated using a "chaotic evolution" that creates a chaotic lattice state based on complicated mathematics--a complicated way of saying that it would make it very difficult for any computer to be able to interpret. Since most online password-hacking systems are automated (and since computers are often unable to interpret CAPTCHAs on their own), they would most likely fail to interpret the second half of the password every single time, especially one designed as complex as this. If you want to see the math on how such a system works then check out the publication at [Cornell University Library](#) (it's free to download).

The researchers say that their method can be "readily and straightforwardly implemented on a wide variety of existing computer systems and devices," and they believe that this technology would be a significant step toward better protecting confidential data whereas current methods may not be as strong. I for one hope that we'll start seeing this technology in Websites like Facebook and Gmail.

The Botnets That Won't Die

Thursday, April 21, 2011

The Botnets That Won't Die

New communications schemes could make zombie PC networks far harder to shut down.

By Kurt Kleiner

Last week the FBI took down the Coreflood botnet—a major network of zombie computers that had been used to steal personal information worth hundreds of thousands of dollars. But the bust relied on an important weakness of conventional botnets—that they are controlled by a few central computers. Take down those central machines and you'll disable the whole network of as many as hundreds of thousands of compromised PCs. Researchers warn that this weakness does not exist in botnets that use peer-to-peer communications protocols, whereby messages are passed from machine to machine instead of coming from a central command.

Peer-to-peer botnets could become more common if coordinated attacks on conventional botnets continue. "When they feel that centralized botnets have more of a tendency to be shut down by the authorities, then they will turn to peer-to-peer botnets," says [Cliff Zou](#), a network security researcher at the University of Central Florida.

A botnet is a network of computers that, unknown to their owners, have been compromised by viruses or worms and can be controlled remotely. Spammers and criminal organizations use them to troll for credit card and bank account information.

Some botnets already implemented have used peer-to-peer communications. Computers in such a network keep a list of peers—other computers in the network—and pass information on to them. When the controller wants to issue a command to the botnet, he inserts it into one or more of the peers, and it gradually spreads throughout the network.

But this design is complicated to implement, and authorities have been able to infiltrate these networks and spread phony commands, files, and peer information, intercepting and disrupting communications.

[Stephan Eidenbenz](#) of Los Alamos National Laboratory and colleagues designed and simulated a botnet that could prove much more resilient. They describe it in an [upcoming paper](#) in *Computer Networks*.

The Botnets That Won't Die

Their hypothetical botnet would randomly configure itself into a hierarchy, with peers accepting commands only from computers higher up in the hierarchy. Any computer taken over by an outsider would thus be less likely to be able to disrupt the network. The botnet would reconfigure its hierarchy every day, so outsiders would have scant time to track down the highest-level computers that could do the most damage.

The technique, together with strong encryption, would make such botnets hard to analyze and attack. "We believe it could be quite effective," Eidenbenz warns.

Zou expects that stronger peer-to-peer botnets are only a matter of time. Once someone writes ways to strengthen a botnet's security into easy-to-implement code, he says, this type of botnet will quickly spread.

But **Brett Stone-Gross**, a computer security researcher at UC Santa Barbara, thinks that even with improvements, peer-to-peer botnets will remain too complicated and vulnerable to being taken over. Besides, he says, conventional botnets remain very hard to battle. "[Conventional] botnets are still the most effective," he says. "They're easy to set up. It really comes down to simplicity vs. complexity. Even if you take down a web server, they'll pop back up somewhere else. You'll see it with Coreflood. It will be back online in a couple of weeks."

Meet the Fastest Public-Key Algorithm Few Have Even Heard of

Meet the fastest public-key algorithm few have even heard of
NTRUEncryption gains X9 acceptance, but is it finally ready for prime time?

By [Ellen Messmer](#), Network World
April 20, 2011 09:36 AM ET

Here comes the fastest public-key algorithm that most people have never heard of: It's called NTRUEncrypt and this month was approved by the financial services standards body, the Accredited Standards Committee X9.

The X9.98 standard specifies how to use NTRU, as it's called for short, in financial transactions.

"The NTRU public-key algorithm competes with RSA and elliptic curve" says Ed Adams, CEO of [Security Innovation](#), which owns the rights and patents associated with the NTRU algorithm. It was invented in the mid-1990s. Unlike RSA, NTRU is not widely used, and in fact the NTRU cryptosystem needed changes early on to improve its security by addressing weaknesses and performance. But today NTRU is recognized as faster than the widely used RSA algorithm.

"It is considerably faster; that is something we acknowledge," says RSA Labs chief scientist Ari Juels.

One study that compared NTRU with both elliptic-curve cryptography and RSA was conducted by researchers at Katholieke Universiteit Leuven In Belgium. "Comparing NTRU to other cryptosystems like RSA and ECC shows that NTRU, at a high security level, is much faster than RSA (around five orders of magnitude) and ECC (around three orders of magnitude)," the researchers said.

Juels argues that the RSA algorithm and cryptosystem, which dates to the 1970s, is a more "mature" public-key crypto technology, having been found to work securely in a time-tested way for many [applications](#).

Meet the Fastest Public-Key Algorithm Few Have Even Heard of

"NTRU hasn't received a lot of scrutiny," Juels says.

Adams fires back that NTRU may be more resistant over time to attack than RSA because NTRU is constructed in what crypto researchers call a "lattice" framework. He claims this type of lattice design makes it more resistant than an algorithm like RSA to so-called quantum-computing attacks. Scientists are continually evaluating the processing power of cutting-edge [quantum computers](#) to determine whether it is possible to break public-key cryptosystems through them.

"A quantum bit assumes multiple values simultaneously and can explore a massive key length," Juels acknowledges. "A quantum computer, if successfully built, would compromise the RSA algorithm and elliptic curve. But it's unclear if it's feasible to construct such a machine."

While such hazy futuristic concerns about public-key systems may worry scientists, it's clear that NTRU has not gained the kind of widespread use in practical applications that RSA has.

Adams does cite a few examples, saying satellite-services provider EchoSat is using NTRU in IP-based payment processing related to Citgo gas stations. Adams also says he is engaged in discussions with [Microsoft](#), McAfee and Symantec on how they might use NTRU in applications such as auto-updates, though no announcements on that score have been made. NTRU may gain more interest from industry later this year if Security Innovation pursues plans to make NTRU available in an open-source model later this summer.

Cyber Identity Strategy Would Eliminate the Need for Multiple Passwords

Cyber identity strategy would eliminate the need for multiple passwords

BY ALIYA STERNSTEIN 04/15/2011

The White House on Friday unveiled guiding principles for industry on developing identity credentials that would allow ID holders to log on to virtually any website, eliminating the need to remember multiple passwords or to enter personal information.

The 52-page [National Strategy for Trusted Identities in Cyberspace](#), first suggested in a 2009 cyberspace policy review ordered by President Obama, represents the start of a public-private partnership to ease online commerce while protecting privacy. Globally, companies conduct \$10 trillion worth of business online, according to federal estimates. The Obama administration opted to house the effort at the Commerce Department, inside an office that acts as a liaison between the federal government and industry.

Federal officials have stressed the ID technology is voluntary. On Friday, Commerce Secretary Gary Locke dismissed rumors that it would be a national ID card or driver's license for the Internet that would enable the government to track citizens' every move online. The strategy calls for adopting standards that limit the kinds of information services can collect. Those standards would stipulates how such data is to be used.

"I'm optimistic that NSTIC will jump-start a range of private sector initiatives to enhance the security of online transactions," Locke said at a launch event the U.S. Chamber of Commerce hosted. "This strategy will leverage the power and imagination of entrepreneurs in the private sector to find uniquely American solutions."

The administration acknowledges the concept -- referred to as an identity ecosystem -- will take many years to implement and require buy-in from international and private sector partners.

Going forward, the role of the federal government in the initiative will be to protect individuals, support industry through workshops and research funding; work with the private sector to ensure the tools are compatible; provide and accept government services using credentials, and lead by example in deploying credential systems internally.

The National Institutes of Health, in coordination with patient advocates and pharmaceutical firms, already has adopted an identity technology to speed the enrollment of patients in clinical trials, including a cancer therapy evaluation program. In the past, paper signatures were required for every stage of the clinical trial approval process, delaying treatment. And passwords were not an option. "Passwords just won't cut it here as they are too insecure and the stakes are too high to risk

Cyber Identity Strategy Would Eliminate the Need for Multiple Passwords

fraud," Locke said.

The technologies should prevent online services from monitoring people's credential use so companies cannot follow their customers' activities online, according to the strategy. The tools would be programmed in such a way that they can be remotely suspended if they fall into the wrong hands. Organizations would have to accept multiple credential formats, similar to how ATM machines accept cards from different banks.

Research shows that, partly because passwords are insecure, 8.1 million American adults were hit by identity theft or fraud last year. For example, hackers employ a practice known as phishing to lure victims into entering passwords, Social Security numbers, bank accounts or other details that can be used to discern passwords on to fake sites that harvest their identities.

Jane Holl Lute, deputy secretary of the [Homeland Security Department](#), who also attended Friday's event, said the aim of NSTIC is not to regulate Internet transactions, but rather engender honesty in online exchanges.

"In cyberspace, can we still trust each other?" she posited. "The goal here is confidence, not centralized control."

The strategy sets out several milestones. For instance, within five years, the program office should develop metrics to measure the progress of the effort, including broad participation, compatibility, choice of a variety of credentials, acceptance at federal agencies, and "trust marks" -- emblems that indicate an organization has complied with the ecosystem's rules. After a decade, the benefits of the ecosystem are supposed to be available to every individual; all policies and technologies are to be in place; a majority of online organizations should be part of the enterprise and a sustainable market for credential providers should emerge.

If the idea of NSTIC is embraced, a person could access secure websites with one so-called trusted identity, which could be stored on, for example, a smart card, key fob or piece of software embedded in a smart phone.

Commerce officials provided the example of a woman who downloads a digital certificate from an ID provider onto her cellphone. She keys in a short password to prove her identity and is then able to conduct from the phone all her online transactions, including paying her taxes. Through such single sign-on mechanisms, a doctor could insert a smart card into his computer to access a federal website after an earthquake and see where medical attention is needed. The site might show that a nearby triage center requires help from a specialist with his background. When he arrives at the center, he could swipe the card to quickly confirm that he is a specialist and start treating victims.

Cyber Identity Strategy Would Eliminate the Need for Multiple Passwords

The strategy was applauded by many in industry who say the administration listened to their advice in crafting the policy.

"If it comes to the point where I can validate and ensure my identity online, and they don't need to know anything except that I have a trusted identity, I don't have to give up any other information; I don't have to give up my mother's maiden name," explained Jennifer Kerber, a vice president of the trade group TechAmerica.

Some privacy groups said they are pleased with the approach the federal government has taken, but the outcome largely depends on the will of industry to follow the rules.

Leslie Harris, president of the Center for Democracy and Technology, a privacy group, said she views the technology as the opposite of a national ID card, because it would hide the individual's personal information. In fact, the current habit of using the same password on multiple sites is just as dangerous as a national ID card because perpetrators who crack a password can then monitor a person's online behavior.

"Now the question is whether industry can step up and enforce a serious governance model in a way that's protective of privacy," she said.

But other civil liberties organizations are more skeptical.

"A top-down strategy for online identity is unlikely to work," said Jim Harper, director of information policy studies at the libertarian Cato Institute. "Trust is not created by government-corporate consensus, but by the hot forge of the marketplace. People will not participate in a government-corporate identity project that deviates from their demand for control of identity information, which is an essential part of privacy protection, autonomy and liberty."

He dismissed the notion that the technology is akin to an online driver's license, however. "People who talk about an Internet driver's license don't know enough about identity systems, the Internet or metaphors," Harper said.

Malware and Other Cyber Threats, Many of Which Are State Sponsored, Are Growing

Malware and other cyber threats, many of which are state sponsored, are growing

BY WILLIAM MATTHEWS 04/20/2011

The wild, wild Web grows ever wilder, and U.S. companies and critical infrastructure remain vulnerable targets, executives from cybersecurity giant McAfee warned Wednesday.

Sixty million malware programs are written annually now, up from 3 million in 2007, McAfee president Dave DeWalt told a conference that included government information technology specialists.

Cyber malefactors are using that malware and other methods to target vital infrastructure, the military, corporate intellectual property and personal identities, McAfee officials said.

Attacks are aimed at virtually anything attached to the Internet -- computer networks, smartphones and other mobile devices, servers, industrial controllers, and even automobiles, some of which are essentially rolling Wi-Fi hot spots, DeWalt said. Other targets include automated teller machines, printers, medical devices and a multitude of other electronic equipment.

The cyber onslaught comes from other nations as well as from organized crime and independent actors, DeWalt said.

At least 20 nations have built cyber vulnerability research laboratories and armed themselves with the ability to carry out cyberattacks, he said. They include nations in Asia, the Middle East, Eastern Europe and Western Europe, DeWalt said, but he declined to name individual countries.

"Countries are investing in a way we've never seen before," and increasingly there is evidence of attacks by foreign governments to steal intellectual property from U.S. companies, he said. "For many years we've seen government on government espionage," but now "there's government on commercial. It's a different landscape."

The statistics collected through McAfee surveys are stunning. One in four consumers has been a victim of digital identity theft, DeWalt said. Increasingly clever spear phishing attacks use personal information, often gleaned from the Internet, to deliver malware embedded in emails that appear to be from friends or bosses.

Keystroke loggers installed unwittingly from infected thumb drives, emails and websites collect passwords that give thieves access to bank accounts and valuable corporate secrets. Root kits -- the

Malware and Other Cyber Threats, Many of Which Are State Sponsored, Are Growing

building blocks for developing malware -- are readily available for sale on the Internet, he said.

Enterprising attackers hand out "candy drops" -- free, but infected, thumb drives, DVDs and other computer peripherals to unsuspecting computer users, who plug them in, inadvertently providing an entryway to otherwise secure networks. In elaborate candy drops, free laptop computers loaded with malware have been delivered to government offices in West Virginia, Vermont and Wyoming.

The cost of the laptop is "peanuts" compared to the value of the information that may be retrieved through them, said George Kurtz, McAfee's worldwide technology chief.

And even when cyber thieves and spies break into networks and fail to find valuable information, they still profit by selling access to those network, he said.

McAfee is developing new defenses against the growing threat, DeWalt said. This summer the company plans to begin offering technology that will reside deeper in a computer's stack of operating software to hunt for malware that has made its way into the operating system or what's known as the BIOS, the basic input/output system. Current antivirus software resides at the application level and does not dig deep enough to protect the OS or BIOS, DeWalt said.

The company also is promoting white listing as a substantial new defense. White listing lets computers access only websites and networks that are preapproved and known to be safe. It is much safer than its opposite, blacklisting, which blocks computers only from sites that are known to be dangerous, DeWalt said.

To determine which sites are safe, McAfee has developed software crawlers that search the Internet and assess whether websites are safe or dangerous, he said.

Is China Winning the Cyber War?

Is China winning the cyber war?

Leaked documents suggest China might have the upper hand

- By [Michael Hardy](#),
- Apr 21, 2011

The Cold War took its name from the relative lack of shooting that characterized it. The United States and Soviet Union fought one another politically, diplomatically and economically but rarely with guns or tanks. It was not a hot war.

We have a couple of hot wars going on now, but there's another cold war under way, too — one being fought between the United States and China, primarily using IT.

And it looks as though China has the upper hand at the moment.

"According to U.S. investigators, China has stolen terabytes of sensitive data, from user names and passwords for State Department computers to designs for multibillion-dollar weapons systems," write **Brian Grow** and **Mark Hosenball** in a report for [Reuters](#). "And Chinese hackers show no signs of letting up."

Grow and Hosenball credit WikiLeaks for revealing many previously secret details about China's ongoing cyber assault, which the U.S. government has code named Byzantine Hades. Specifically, they write, the State Department cables that WikiLeaks published show that the Chinese military was the source of those attacks, not some rogue hacker group.

Responding to the Reuters report, **Adam Martin**, blogging for [The Atlantic](#), said: "In short, the Chinese are way better at cyber spying than pretty much anybody else."

However, he dismisses the idea that cyber spying is a serious threat to U.S. national security. "The Chinese are unlikely to invade any time soon, even if they find out when the secretary of Defense takes his lunch break," Martin writes. "Rather, the attacks are one of many tactics China is employing to keep its economy growing." Chinese cyberattacks have also targeted private businesses, and news reports detailing individual intrusions are plentiful, he said.

Collin Spears, a blogger for the [Foreign Policy Association](#), read the situation the same way.

Is China Winning the Cyber War?

"The infamous 'Google E-mail Hacks' of 2010 are a case [in] point," Spears writes. "Google openly implicated China in an e-mail hacking scandal, but this situation is actually not uncommon. It is just that Google went public and garnered significant media attention due to its status."

Spears notes that more than 34 other companies, including technology and defense firms, are believed to have been cyber targets.

But **William Jasper**, writing in the [New American](#), takes a dimmer view of China's motives. Although some experts think China might not be the perpetrator but instead the victim of outside forces hacking its poorly defended systems and using them to stage attacks, those arguments are unsupported, Jasper writes.

People who feared Soviet infiltration of the United States during the Cold War have been proven correct in at least some instances, Jasper writes. "The arrests in the past months of Russian and Chinese spies in the United States provide ample evidence that the communist propensity for espionage and deception has not abated among the supposedly 'reformed' leadership of the Beijing regime."

Jasper and others also point out that the cyberattacks haven't been trivial test runs. Chinese hackers penetrated Defense Department computers and gained access to material on the Joint Strike Fighter program. Chinese hackers have also apparently penetrated the United States' energy grid and left behind software that could be used to disable the grid remotely, the [Wall Street Journal](#) reports.

The concerns are not new. In September 2007, the [Times of London](#) published an article headlined, "China's cyber army is preparing to march on America, says Pentagon." Reporter **Tim Reid** said U.S. military officials believed that the Chinese military had a detailed plan "to disable America's aircraft battle carrier fleet with a devastating cyberattack."

About the Author

Michael Hardy is the managing editor/daily report for the 1105 Government Information Group.

Network Would Link Defense Functions, People

Network Would Link Defense Functions, People

(AMERICAN FORCES PRESS SERVICE 25 APR 11) ... Terri Moon Cronk

WASHINGTON, April 25, 2011 - To optimize U.S. cybersecurity using a new information-sharing enterprise network in a reduced-budget era, a top Defense Department official gave industry leaders a challenge: "We need your innovation."

Robert J. Carey, deputy assistant secretary of defense for information management integration and technology and the Pentagon's chief information officer, outlined the department's "enterprise strategy and roadmap" for members of the Armed Forces Communications and Electronic Association here April 22.

Carey said the plan would bring all branches of the military together on the same information-sharing network system.

"It's not about consolidation as much as it is about raising security, while keeping enterprise in view," he said. "Improving cybersecurity is what this is about."

Making sure firewalls get trusted information and driving costs down while raising the security bar form the nexus of the effort, Carey said.

"When a service member is downrange, he doesn't care where the information comes from — only that it's at hand and he can do something with it," Carey said. "Enterprise is actionable, timely, relevant, trusted information."

And while it seems simple to provide, he said, the existence of many networks makes it difficult.

Defense budget cuts have become the catalyst for change, Carey told the industry leaders, and finding efficiencies to run the department has become essential.

"If we keep doing what we've done [with past funding], we're not going to get there," he said.

The enterprise network, however, would cost little, because the system's architecture would result from a "bottom-up" approach, Carey said, with DOD making new uses out of existing network equipment from all military branches.

"It's really hard to defend [the department's] 15,000-ish networks and 10,000 applications and systems," he acknowledged. But even with a substantial amount of details yet to be ironed out — including network optimization, data center consolidation, data tagging and others -- Carey said some efficiency initiatives already are paying off after six to eight months of work, such as in tracking identity on classified networks.

"It's actually starting to happen," he said.

Email is another challenge. "There are a lot of email systems out there," he told the group. "We've got to buy what we have better, and use what we have better."

Carey said all branches of the military bought email systems and set them up command by command, ship by ship, with no tightly knit communications system. But now, he added, enterprise system purchases for hardware and software will be viewed with a critical eye.

"We need to look at: 'Is it applicable at the enterprise level? If it is, how can I buy it better than I'm buying it now? How can I use my money more wisely for the taxpayer?'" Carey said.

Network Would Link Defense Functions, People

The challenges of the new enterprise system will be many, Carey said, but he added that he believes it is a proven system that is both cost-effective and essential for improved cybersecurity.

"We are starting this pump with the water we already have," he said, noting the drop in funding for the enterprise network system. "And the defense leadership recognizes that factor."

Launching the system will take more time with less funding, Carey said, "but we're still going forward, because this can be done on its own gravity."

Inside the Army's App Store for War

First Look: Inside the Army's App Store for War

- By [Spencer Ackerman](#)  April 27, 2011 | 7:00 am | Categories: [Army and Marines](#)



If all of the bureaucratic and security hurdles can be overcome, the Army will soon launch its version of an app store, where soldiers can download Army-relevant software to their work computers and — with a little luck — mobile phones. This is what its homepage will look like.

Called Army Marketplace, it'll start off featuring the few dozen applications that soldiers created last year during the [Apps for the Army contest](#). Those early efforts ran the

Inside the Army's App Store for War

gamut from workout guides to digitized manuals for standard Army tasks. So far, there are 17 apps for Android phones and another 16 for iPhones.

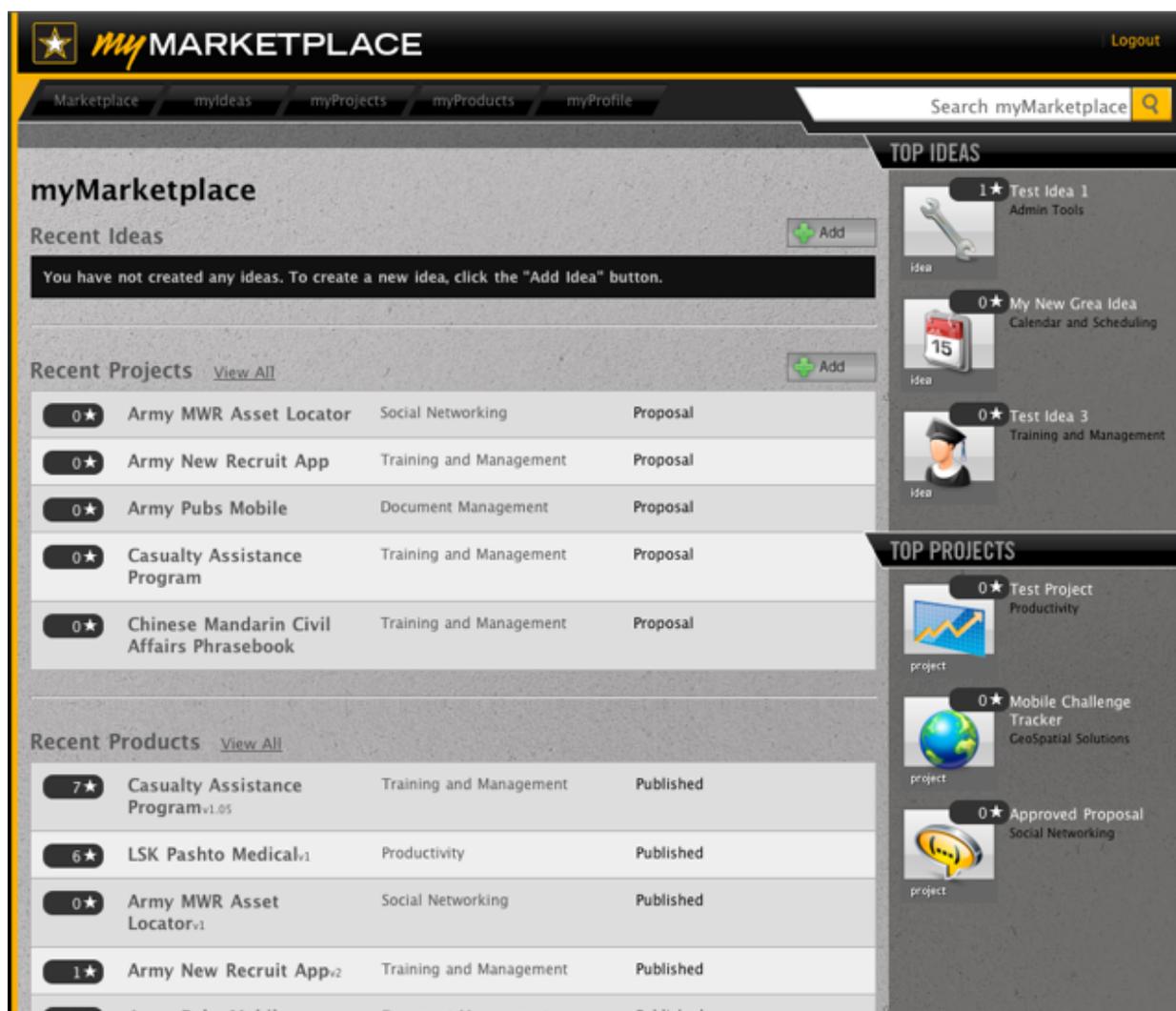
But the Army Marketplace will do more than sell existing apps. It'll help generate ideas for new ones, says Lt. Col. Gregory Motes, chief of the Army's new Mobile Applications Branch. Imagine that a soldier wants an app instructing how to call for artillery fire, and the app doesn't exist yet. The soldier would post a description of what she needs on a Marketplace forum, attracting discussion from fellow soldiers and potential designers.

If other troops can't home-brew a solution, the Army would open a bidding or contracting process from would-be vendors who've expressed interest on the thread. Ideally, the app would be available on Marketplace not long thereafter, with a nominal purchase price, a la the App Store or Android Market.

"It'd use an agile software-development process, to close with the vendor and try to quickly turn these apps around," Motes tells Danger Room. "The current process of software creation [in the Army] is a very long and arduous process. That's how we do things. But app development needs to be done quickly."

You'll have to be a member of the Department of Defense community to see the store and access its wares. It'll be hosted on a secure DOD server and require a username and password from intranets like [Army Knowledge Online](#). Eventually, Marketplace will become an app of its own, loadable onto the forthcoming Army-issued smartphone so users aren't tied to a website. Marketplace isn't meant for the general public — which creates problems for how it interacts with smartphones. (More on that in a moment.)

Inside the Army's App Store for War



Army Marketplace’s designers are also working on personalized user pages to facilitate the app exchange. On them, customers announce their needed apps, propose new ones, and exchange criticism. On the right hand side of that inside page are auto-generated lists of “Top Ideas” and “Top Projects” that others have generated. (That’s a screenshot of a personalized page, above.)

Army brass like Gen. Peter Chiarelli, the vice chief of staff often seen thumbing like mad on his iPhone 4, view apps as a game-changing approach to [pushing information down to the lowest ranks](#) and exponentially increasing the Army’s ability to learn and adapt. So the service has set up new shops — like Motes’ parent organization, called

Inside the Army's App Store for War

Connecting Soldiers to Digital Applications — inside the Army's Training and Doctrine Command, to help generate an ecosystem of military-friendly applications.

Eventually, the Army will host apps that [track the location of friendly forces](#) or [map out wartime terrain](#) or [translate foreign languages](#). Software writers and defense companies have already created all of those. On top of that, the Army will launch its second Apps for the Army contest later this year as a way to generate both more apps and a constituency for them inside the service.

There's just one small problem. The government hasn't certified any single mobile device as secure enough to receive data from its networks. If all goes according to plan, the Army will unveil Marketplace in August, at the [LandWarNet convention](#). That'll mean whatever applications are currently available could be easily sent to a soldier's work computer — which doesn't really help, given the whole idea is to allow mobile access to the corpus of Army information.

The Army's now testing Google's Android OS to [power its first smartphone prototype](#). That's made by MITRE, the federally funded defense consultancy. Other defense companies use Android's open architecture as the backbone of their own mobile devices that they'd like to sell the Army, such as [Raytheon's RATS](#) and [General Dynamics' GD300](#). But the Army isn't near close to settling on an operating system or a mobile device for its ultimate goal of requiring soldiers to carry a smartphone just as they carry a rifle.

And no Android phone has so much as started going through the process of having the National Institute of Standards and Technology certify it as secure-enough to host government data. The iPhone has started the process, Motes says, but is still months away from finishing it.

That's why government BlackBerries can process someone's official mail and do

Inside the Army's App Store for War

practically nothing else a civilian smartphone does. As of now, “we don’t have a solution for authenticating applications or secure websites,” Motes says.

How long until a phone receives certification? “An optimist might say 12 months,” Motes assesses, but being pragmatic, it’s further down the road.”

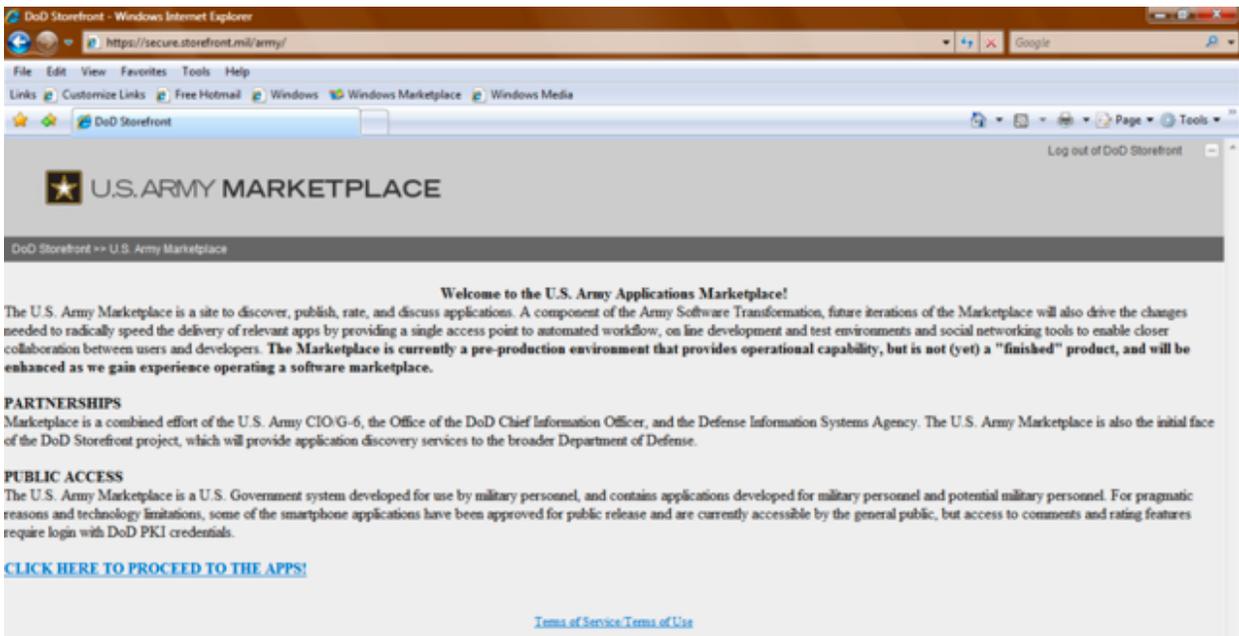
Until then, Marketplace will be a good place to download web apps and dream up apps of the future. It won’t be useful for loading up your phone with Army apps.

But it’s possible, Motes says, that “commanders can take risks” if they can convince the Army there’s a pressing need in a “tactical environment” for skipping certification. Welcome to the laborious process of getting the Army prepared for the day when every soldier is required to carry a secured smartphone.

That’s not the only challenge. Congress’ inability to pass a budget for months set back the apps program. A LandWarNet debut for Marketplace remains the goal, Motes says, and “if they don’t announce at LandWarNet, then it’s just a big sigh.” Another headache is securing the apps themselves, a process of going through code “line by line” looking for potential security flaws, which “is gonna drive us crazy.”

But at least Motes is convinced that at the end of this process is an agile website and mobile portal that will connect soldiers to apps that will let them do their jobs better. It’s a lot more functional and intuitive than the laughable attempt at a placeholder homepage for the Apps for the Army results, called Storefront, currently hosted at storefront.mil/army:

Inside the Army's App Store for War



Motes sums up Storefront in one word: "Busted." Now to see if Marketplace will fix it.

Pentagon Taps EW for Second Wind

Pentagon Taps EW For Second Wind

(*AVIATION WEEK 27 APR 11*) ... David A. Fulghum

The U.S. has been falling behind in the arena of electronic warfare—a key element in defeating enemy air defenses—for perhaps the last 20 years.

That may explain why the Obama administration—while it is looking for further military cuts—has chosen electronic warfare (EW) as one of the few areas slated to receive a spending boost, says Frank Kendall, deputy undersecretary of defense for acquisition and technology.

“We’ve not invested in the EW side of the house recently as we should be inclined to do,” Kendall says. “I would say it will receive increased emphasis as our focus shifts” to squeezing more costs out of the defense budget.

The Pentagon’s decision to retire the U.S. Air Force’s EF-111 EW and tactical jamming aircraft in May 1998 augured the beginning of the downturn. After just a few years, U-2s flying over northern Iraq were being threatened by air defenses that they were not aware existed. The reason that threat updates made by the Navy were not being passed on to the operational Air Force was because the latter’s EW community had been dispersed and there were no high-ranking advocates of the technology in senior leadership positions.

The retirement of the EF-111 and shifting EW responsibilities to the Navy comprised a piece of the equation, but Kendall is unsure whether it was the dominant factor.

“We used to regard ourselves as much more competitive in the EW environment than we have been in the last decade or two,” he says. “Our capabilities and the degree to which we are ahead of the [threat] power curve has atrophied. We have to take a look at that and get our strength back.

“I used to have the EW shop back in the late 1980s and early 1990s for [the Office of the Secretary of Defense] and we had a pretty robust program with a lot of products under development,” says Kendall. “We understood that we were in a game that kept going, and that you have to keep making advances continuously to stay ahead. We’ve gotten complacent since then. Some of it was due to force structure consolidation.

“I think we’re starting at this point to revitalize that field,” he adds.

Directed energy—such as high-energy lasers and high-power microwave weapons—may not fare as well, at least in the near term.

“Directed energy is one of those technologies that is always five years away,” Kendall says. “In the 1980s I was doing missile defense work for the Army, and at that time we were talking about directed energy being a few years away. There have been great advances in the technology, but there are still steps to be taken before we have practical weapons. When people ask what we want, the answer is affordable, executable [new] programs. In addition, we’re trying to get cost out of [existing] programs.”

The plan to resuscitate EW comes as the U.S. has arrived at the intersection of intelligence, surveillance and reconnaissance (ISR), directed energy, cyberoperations and the need for electromagnetic battlefield management (EMBM). The electronic pollution in Baghdad, for example, produced an environment where turning on a new piece of equipment nearly always

Pentagon Taps EW for Second Wind

jammed something else. In Afghanistan, electronic management has improved but is still a problem.

“We’ve gotten much better at electronic de-confliction since we started operations in Baghdad in 2003,” says Lt. Gen. (ret.) Dave Deptula, who was chief of U.S. Air Force intelligence and ISR. Moreover, “with cyber being part of the planning process, there needs to be de-confliction with organizations capitalizing on operations in the cyberdomain. We tended not to do that kind of integration in the past. As a result, people were [electronically] stepping on one another. It was less bad when we did the buildup in Afghanistan.”

The Air Force is embracing the concept of adapting existing aerospace system by linking them in a way that creates new effects. Such linkages exploit integration of the various technologies carried on each platform. This leads the services away from packaging forces by using large numbers of specialized aircraft.

“With low-observable, fifth-generation aircraft carrying highly capable ISR, you can do things we’ve never been able to do before—such as putting out a network of aircraft so that if you lose a percentage of them, the rest of the force maintains its effectiveness,” says Deptula. “As we normalize cyberoperations as part of a warfighter commander’s toolbox—and get away from central control only by U.S. Central Command—we’ll be able to expand on some of these technologies that are available to us.”

Again, organizing and integrating these technologies will be a big problem. Already under consideration by the U.S. Navy is EMBM that will rationalize electronic warfare just as in air-to-air combat (AW&ST April 18, p. 18).

“We have to make sure [EMBM] doesn’t come with lots of layers,” says Deptula. “It’s exactly what needs to be done, but in order to put that kind of architecture in place, you need a fresh look at our whole air operations center concept. It’s now 20-plus years old. We need to move away from large, ponderous, centrally located facilities to distributed command-and-control processes that are much more flexible but still able to address the entire set of existing capabilities.

“There are going to be all kinds of parts and pieces that need to be orchestrated, and that need to be integrated with a plan for the effects you want to create,” he says. “Aircraft like the F-22 are flying sensor and electronic attack platforms that we need to capitalize on. We need to link all our fifth-generation [platforms] so that we can create this honeycomb of capability that we can put wherever we want.”

Two areas of spending and technology advances are linked to this vision for the Defense Department’s financial and operational future—information technology and the Lockheed Martin F-35 Joint Strike Fighter. They will be prime targets for budget cutting and therefore likely political battlegrounds.

“We can always buy less,” Kendall declares. “The question is, what do you give up? We are at a point where we’ve got to make tough decisions about what risk we will accept, what mission capabilities we will have less of and [what we can] do less of [operationally] in the world.”

There will be a roles-and-missions review soon and yet another major review of F-35 costs that could affect the budget and force structure.

Pentagon Taps EW for Second Wind

Kendall first wants a discussion with the Government Accountability Office about how it measures cost growth. He contends that GAO's first-order analysis uses pretty crude metrics. Therefore, the first big cost number draws the most attention while, later, refined GAO assessments are ignored.

"Programs get in trouble; and when they do, they tend to attract fire," Kendall says. "That doesn't necessarily say their value is diminished. You still want the capability."

The Joint Strike Fighter has had its share of problems, Kendall observes. The short-takeoff-and-vertical-landing (Stovl) version has been a key element in that turmoil, as well as the mission software. But he notes that the aircraft "is also our highest priority."

Options are to accept less capability on the platform, which means more operational risk, he says. Killing a program often just means starting over while losing the initial investment.

"We see progress [with the F-35 program], but not as much as we would like," says Kendall. "Stovl is a question mark because of design issues. The program is maturing. The first production aircraft is flying. I don't like to be an optimist about programs. But I do think that in the case of the F-35, we're getting it under control."

Meanwhile, upgrading information technology has its own set of unique cost-estimate problems.

"When I came in, I started trying to find people in the building who understood these systems," he says. "There are classic problems like not having enough expertise on board to do things smartly. We also discovered that economies of scale have limitations. Something of that size creates a lot of complexity."

Government regulation requirements are another source of complexity, he adds. "On a certain IT system, there were 170,000 compliance requirements that had to be implemented into the software. You don't just take an off-the-shelf product and use it. The biggest problem we've had is trying to do too much too fast and not breaking the jobs up into manageable bites with well-defined requirements that are testable and that you can then cost well" in order to make accurate predictions.

DoD Urged to Rethink Acquisition Managers

DoD Urged To Rethink Acquisition Managers

(DEFENSE NEWS 02 MAY 11) ... Andrew Tilghman and Marcus Weisgerber

The Defense Department should change how it picks the program managers who handle large contracts and development programs, a Pentagon advisory board has recommended.

A review by the influential Defense Business Board criticized the system that puts majors and lieutenant commanders with little or no business background in charge of an estimated \$400 billion in annual contracts.

The Pentagon should either "professionalize" the uniformed acquisition corps or "civilianize" the program management's leadership, according to recommendations approved at the board's April 21 meeting.

DoD should consider creating a career field with a separate promotion board for program managers and expand education programs for service members who want to focus on acquisitions, the board said.

"Make it a job, not a tour. A career destination," said Fred Cook, a businessman and board member who led the review.

Military program managers often do not have a background in making cost, schedule and performance decisions, according to Richard Sylvester, a former Office of the Secretary of Defense official with decades of acquisition experience. While all program officials go through training at Defense Acquisition University, there is no substitute for experience.

"There's a difference between learning something and actually having lived it," said Sylvester, who now works for the Aerospace Industrial Association (AIA) but who spoke on his own behalf. AIA has not taken a position on the recommendations.

"My experience when I was at DoD was, those people that had been through more than one program were much better the second time around than they were the first time around," he said.

Nearly 150,000 people make up the defense acquisition work force, including hundreds of program managers, according to a Pentagon spokeswoman.

The board discussed, but stopped short of recommending, the creation of a new military command for acquisitions.

The Air Force already has created an acquisitions force similar to the one the board is recommending for the entire military. The service's weapon buyers are part of a program management career field.

One problem with the system is that many large programs can take 10 or more years to complete, but program managers rarely remain in their position for more than four years. And during that time they often get pulled away for deployments, temporary duties or professional development.

"The challenge is, getting somebody in those positions that has enough experience to be able to manage well," Sylvester said. "The services have always wanted military people because they think that it's better to have a guy with a uniform on dealing with the requirements side of the service."

This way when a program manager and requirements official interact, it will be military-to-

DoD Urged to Rethink Acquisition Managers

military. The military thinks this approach gives the program manager a better sense of what operators desire because they've previously served on the battlefield.

"You certainly have a lot of command authority when you have a uniform on, so having some of each is probably the desirable thing," said Jacques Gansler, who served as the Pentagon's acquisition executive in the Clinton administration.

Program managers also make short-term decisions and are risk-averse, board members said. They tend to put off tough issues, delaying big decisions — and problems — so the next program manager has to deal with them, the Defense Business Board said.

"With the length of these acquisition programs, you don't have to live with the decisions that you make, somebody else has to live with them," Sylvester said.

On the same subject, Cook said: "If you're going to be there two more years and you're looking toward your next assignment, it's natural."

The review also found that too many Pentagon offices have authority to alter or change a program's design or demands. That forces program managers to essentially oversee "a political process to make sure the approval process continues," he said.

The internal review began in December when Ashton Carter, acquisition defense undersecretary, asked the board to identify "best business practices that could improve the intake and development of military acquisition program managers."

The Defense Business Board is an influential advisory panel that helped Defense Secretary Robert Gates develop many of his "efficiency" initiatives in recent years.

Concern about program managers is a problem the Pentagon has wrestled with for years and recommendations — like the ones presented by the board — have been talked about since the 1980s. The Goldwater-Nichols Act, written in the 1980s, requires a military official to have experience in a program management area, such as serving as a deputy program manager, before leading a program, Gansler said.

"That is an important consideration because you don't want somebody just because they have been a tank driver to necessarily be running a tank program," he said. "You do want to have inputs from the operator side and you often would like to have somebody in your office with operator experience, but the management of the program should be someone who has management experience."

In 2005, the Government Accountability Office (GAO) identified similar concerns. In 2007, Congress ordered the Defense Department to develop a "comprehensive strategy for enhancing the role of DoD program managers."

"If history is any judge, the over-all environment within which program managers perform their work is very difficult to change simply with policy initiatives," the GAO concluded in a 2007 report. "Unless all of the players involved with acquisitions ... are unified in implementing these new policies from top to bottom, they will be for naught."

Army Enlists Android for Battlefield Comms

APRIL 21, 2011 2:01 PM PDT

Army enlists Android for battlefield comms

by [Don Reisinger](#)



During an exercise at Fort Bragg, N.C., in early March, members of the 82nd Airborne made use of both standard-issue radios and prototypes of Android-based smartphones.

(Credit: U.S. Army/Ashley Blumenfeld, JPEO JTRS)

The U.S. Army is establishing a beachhead on the shores of smartphone tech, and it's got Google's Android operating system in its ranks.

The Android-based Joint Battle Command-Platform (JBC-P) gadget is undergoing evaluations and moving closer to deployment, according to a [report on the Army Web site](#) earlier this week. The JBC-P Handheld, which is currently in prototype form, is part of a broader effort by the Army to bring more mobile communications capabilities to soldiers engaged in tactical operations.

It's a significantly modified version of Android, called Mobile/Handheld Computing Environment, that's running in the JBC-P Handheld. The Army is supplementing the platform with several mission command applications, including mapping, blue force tracking, tactical ground reporting, and critical messaging. In addition, soldiers will likely have access to other applications including an address book and Open Office.



Over the summer, the Army plans to release a software development kit for third-party developers to create other applications that might be of use to soldiers. The applications built into the platform can be enhanced by third-party developers, as well, the Army.mil report says.

"It's like when you get an [iPhone](#) and you have the Apple-made apps: the contacts, the e-mail," J. Tyler Barton, an engineer working with app makers in the Army Research, Development, and Command division, said in the report. "Then other applications are free to use those apps, or to go above and beyond that."

Army Enlists Android for Battlefield Comms

Having this sort of handheld on the front lines could be a boon for soldiers, the Army claims. It cited one implementation where a soldier on a field exercise input locations of enemies and roadside bombs into the device, which was then accessible from handhelds of other soldiers who might be traveling through that area. The Army also designed the platform to make it easier for soldiers to track others in their own units.

The Army has a number of pilot programs going to evaluate smartphone technology (not limited to Android), for both operational and training uses, and in both secure and unsecured environments. Earlier this year, Lt. Gen. Michael Vane, director of the Army Capabilities Integration Center, pointed out to a blogger roundtable that the people that U.S. soldiers are fighting have had a great deal of success using cell phones generally.

"One of the most significant feedbacks you get from soldiers in theater is they look at their Afghan army compatriots or the Taliban guy, who has a cell phone, and then the Army guy looks at his MBITR or his 117G radio, and we want to deny that capability to our own Soldiers even through the enemy is using them?" Vane asked, according to an [Army News Service](#) report in February.

In early March, after watching members of the 82nd Airborne Division make use of the Android-based smartphones in conjunction with standard tactical radios, the Army's vice chief of staff offered praise for the technological capabilities.

"What I watched with interest today was the ability to take pictures of high-value targets, immediately provide them to the company or to the battalion command post," Gen. Peter Chiarelli [said](#). "I saw the ability when a soldier is wounded to take a picture of the wound and to pass that to the doctors, so that medics can make sure that they are treating the soldier in the appropriate way, given the wound that he has received. So there are many, many applications of this."

Meanwhile, it's going to take some time before the JBC-P Handheld is actually in the hands of U.S. soldiers in real-world missions. The Army doesn't expect it to be fielded to its people--or to the Marine Corps--until the government's 2013 fiscal year.

Five Navy Commands Realigned to Cyber Command in Maryland

Five Navy Commands Realigned To Cyber Command In Maryland

(VIRGINIAN-PILOT 18 APR 11) ... Kate Wiltrout

Five local Navy commands transferred today into a new command structure.

Navy Information Operations Command, Naval Network Warfare Command, Navy Cyber Defense Operations Command and Naval Computer and Telecommunications Area Master Station Atlantic were administratively realigned and now belong to Fleet Cyber Command at Fort Meade, Md. They had belonged to Navy Cyber Forces, which is headquartered at Joint Expeditionary Base-Little Creek in Virginia Beach.

The workforce at Forces Surveillance Support Center in Chesapeake, which includes about 300 civilians and contractors, was also realigned to Fleet Cyber Command.

The five commands had already reported to U.S. Fleet Cyber Command at Fort Meade for operational purposes. Today's change means Fleet Cyber Command now handles their administrative issues as well. Fort Meade is also home to the National Security Agency.

Cmdr. Steven Mavica, a spokesman for the cyber command, said there are no plans at this point to move any personnel to Fort Meade, but some vacant positions might be shifted to Maryland and filled from there.

Vice Adm. Barry McCullough, Commander, Fleet Cyber Command/U.S. Tenth Fleet, said in a Navy news release that the realignment will provide the command and control structure necessary to achieve "decision superiority" in the information domain.

ONR's Digital Tutors Give Naval Recruits, High School Students An Academic Edge

ONR's Digital Tutors Give Naval Recruits, High School Students An Academic Edge
(PHYSORG.COM 18 APR 11) ... Office of Naval Research

When President Obama underscored the importance of a college education to eighth-graders during their April 11 visit to the White House, he was echoing the collective sentiment among the nation's educators and organizations that graduates must be prepared for the world's technological challenges and opportunities.

The Office of Naval Research (ONR) may have a hand in helping that class of 2015, and others, make the grade with computer-based applications similar to programs originally designed for Navy recruits.

Playing a 3-D video game developed by ONR, the science and technology provider for the U.S. Navy and Marine Corps, recruits are learning at-sea safety long before setting sail. And now, applying the same underlying science in public education, digital tutors are helping high-school students to master math.

Program Officer Dr. Ray Perez leads ONR's Cognitive Science of Learning program. In collaboration with the Naval Service Training Command (NSTC) and a team of academic researchers, Perez and his colleagues are developing advanced training and education techniques with significant cost savings for the U.S. Navy.

"Training and education are national defense priorities," Perez said. "We're seeing an influx of recruits who are not as well equipped to handle the technological complexities of today's Navy, and we cannot wait for the standard education practices to fix that."

Virtual Learning Helps Recruits Retain Skills

Since fires and floods present the greatest threats on a ship or submarine, each recruit must complete training on containing a fire, controlling a flood and rescuing personnel during their initial seven-week boot camp. On completion, learned skills must be demonstrated on a capstone event or exam. For those who fail, it's back for another round of training.

NSTC Great Lakes employs computer-based simulations to measure individual performance and help recruits prepare for their final assessment. The first-person game emphasizes operational

ONR's Digital Tutors Give Naval Recruits, High School Students An Academic Edge

skills relating to flood and fire control and preventing casualties aboard ship – a critical skill in helping trainees to earn their sea legs.

"During the game, users are given real-time feedback on their performance as well as guided instruction when they run into different challenges or have difficulty obtaining individual objectives," said John Drake, director of learning sciences at NSTC.

The results speak for themselves: After gaming, recruits make 50 percent fewer errors, and locate ship or submarine compartments in 50 percent less time. In a study measuring how much information recruits retain after boot camp, game-playing recruits retained 83 percent of their reading gains, almost four times more than their counterparts.

Drake attributes improved scores to the appeal of video games among men and women who have grown up with consoles such as Nintendo, Xbox and PlayStation.

"They seem to align better with the learning preferences of this generation and be the next step in the direction that training needs to go," Drake said.

Among competitive trainees, the game has evolved into an extracurricular opportunity to excel.

"What we find is that during off-duty time, recruits play the game," Perez said. "You get points for how well you perform your tasks. For example, at NSTC Great Lakes, dormitories compete to see who gets the highest score."

At NSTC, computer-based games focus on teaching recruits their individual roles in a crisis situation, but it's equally important that seasoned Sailors learn and refresh on operating in a team setting.

Working with the National Center for Research on Evaluation, Standards and Student Testing at the University of California, Los Angeles (CRESST/UCLA), ONR has developed the Damage Control game to prepare Sailors for deployment. Currently in use at the Center for Naval Engineering in Norfolk, the simulation teaches Sailors what actions to take, and with which people and equipment at the appropriate time.

"The goal for the player is to manage what's called the 'repair locker,' a collection of people who are responsible — like a fire department — for responding to different fires or floods that may break out in that particular area of the ship," said Alan Koenig, CRESST/UCLA senior researcher."

ONR's Digital Tutors Give Naval Recruits, High School Students An Academic Edge

Real-Time Learning Analysis

While its ability to engage players is one factor in its success against more traditional learning exercises, Damage Control's built-in analyses tools rate equally as high among instructors and evaluators.

During play, the computer measures anxiety levels based on data retrieved from electronic sensors attached to the recruit. As students experience difficulty or frustration, the game reverts back to more basic tasks before advancing too far ahead. The game is continuously adjusting difficulty levels based on the player's ability.

The game allows players to assume different roles — such as repair locker leader, investigator and fire team member — and gives them access to casualty checklists that update automatically based on their actions.

Damage Control offers real-time feedback and captures data for reporting and future enhancement purposes. The game's back-end leverages graphic models of the relationships and probabilities among concepts and procedures that are critical to completion of the task. The computer-based game is integrated with the network in real time to provide analysis for after-action review. Performance data is reviewed post-game to measure proficiencies and can be displayed in multiple formats, including charts, curve graphs and checklists. The data are analyzed both within game and across games (over time) to model changes in knowledge, skills and abilities in key areas.

"More Without More"

The one-on-one instruction afforded by computer-based games is proving not only effective, but also economical. These applications save instructor expenses as well as overhead costs, such as building maintenance and classroom materials, since the instruction can take place almost anywhere.

Additionally, ONR seeks to lessen the cost of digital tutor development by working with partners to develop game-authoring tools. These products would enable the development of new games at a fraction of the cost and time while allowing the Navy to emphasize quality in education.

Currently reviewing Small Business Innovation Research (SBIR) proposals, Perez sees these tools as a means to counter the shrinking numbers of qualified naval instructors due to retirement

ONR's Digital Tutors Give Naval Recruits, High School Students An Academic Edge

and attrition.

"Ideally, in the future, it could be that we have these games available to recruits as they come in to lessen the time it takes them to learn some basic information; but more importantly, lessen the time for them to become experts," he said.

Applying Naval Science to High School Learning

The use of similar technologies may have wider implications within the public school system. ONR-sponsored researchers at Arizona State University have demonstrated the success of digital tutors among algebra students at Mountain Point High School, raising student grade levels.

"Using digital training standardizes what kids learn, and can increase learning by one third and do it in one third less time and at one third the cost," Perez said.

From the Navy's perspective, digital media could also lure students toward science, technology, engineering and mathematics (STEM) disciplines and provide them with critically needed technical skills that are important to the Navy. These one-on-one digital tutors and learning games could boost learning achievement in the Department of Defense Education Activity (DoDEA) schools, in keeping with Presidential Study Directive 9.

In response to the directive, the January 2011 "Strengthening our Military Families: Meeting America's Commitment" report proposes new measures to improve the quality of life for service members and their families. The Defense Department has pledged to boost educational excellence in military schools by investing in research, development and demonstration projects. The move, which supports one of four priorities outlined in the report, could advance DoDEA schools as leaders in advanced learning technologies.

Taking the STEM lead for the U.S. Navy, ONR will host the 2011 Naval STEM Forum in June, where cognitive learning sciences and educational initiatives – including computer-based training – will fuel an ambitious agenda.

However it is used, computer-based training is opening new possibilities for the Navy and beyond. Senior researcher Koenig predicts, "The ONR emphasis on this particular project is really quite groundbreaking. It will open doors for a lot of great things in the future."

Bin Laden's Computers Will Test US Forensics

MAY 6, 2011 4:00 AM PDT

Bin Laden's computers will test U.S. forensics

by [Declan McCullagh](#)

For the U.S. government, the raid on Osama bin Laden's compound in Pakistan represents a unique opportunity to test advanced computer forensics techniques called "media exploitation" that it's developed over the last few years.

The military's acronym for the process is DOMEX, which one Army team in Iraq cheekily sums up with this motto: "You check their pulse, we'll check their pockets."

The electronic gear hauled away by an assault team of Navy SEALs reportedly included five computers, 10 hard drives, and scores of removable media including USB sticks and DVDs. Some reports [say](#) the forensic analysis is taking place at the CIA's headquarters in Langley, Va., while others [have placed it](#) at a "secret location in Afghanistan." (See [list of related CNET stories](#).)

While the U.S. government isn't exactly volunteering what's happening now, the Army has confirmed in the past that it provides "tactical DOMEX teams" to troops in Afghanistan. And a Defense Department directive ([PDF](#)) from January 2011 says the National Media Exploitation Center, or NMEC, will be the "central DoD clearinghouse for processing DoD-collected documents and media," a category that would include the bin Laden files.

Like the National Security Agency in the 1970s, the NMEC isn't a very visible organization. It doesn't have a public Web site. It's intentionally low-profile, and it prefers to stay that way.

The NMEC falls under the [director of National Intelligence](#) and is responsible for "the rapid collection, processing, exploitation, dissemination, and sharing of all acquired and seized media," including forensic analysis, translation, and dissemination. It's overseen by Dan Butler, DNI assistant deputy director for open source, a former Naval intelligence officer.

After NMEC obtained the bin Laden files, which could have happened within hours of the raid, they would have been uploaded to its HARMONY database, which is intended to be the master repository for "documents and media captured or collected to support the global war on terrorism." West Point's Combating Terrorism Center [has used al Qaeda documents](#)--extracted from HARMONY and declassified--to analyze why the group failed in Iraq.

An initial forensic analysis of bin Laden's hard drives will likely be done with keyword searches in Arabic and English. "You can get thousands of hits," Mark McLaughlin, president of Santa Monica, Calif.-based [Computer Forensics International](#), told CNET. "Those hits need to be looked at individually, and in context," he said, which can take a while.

U.S. officials are calling the data a potential treasure trove of information on al Qaeda's current and planned operations, perhaps the most important since 9/11. They're hoping it could yield hints

Bin Laden's Computers Will Test US Forensics

about the whereabouts of Ayman al-Zawahiri, bin Laden's chief lieutenant.

Denis McDonough, the deputy national security advisor, has said the electronic haul is "probably going to be impressive," and White House counterterrorism advisor John Brennan told CBS' Early Show that "what we're trying to do now is to understand what he has been involved in over the past several years (and) exploit whatever information we were able to get at the compound." (CBS News is CNET's sister news organization.)

While government officials aren't exactly sharing details about their approach, McLaughlin believes that they'll be using Guidance Software's EnCase utility, arguably the market leader in forensics analysis. "They're making copies of all the evidence," he says. "Then they'll parcel out the work to the different examiners. You'll undelete everything you can. If there's any encryption you have to deal with, you'll handle it."

Then, he says, it's time to reconstruct what happened. "Were files created at the same time? Were they out there searching the Web at the same time? You can put these together and draw correlations."

Another forensics tool that might come in handy: Vound's Intella software, which helps sort through reams of e-mail. It's [marketed to law enforcement](#) as "searching email by keywords, or senders/recipients, easily viewing search results through cluster mapping, or quickly viewing email threads." (Most reports say that bin Laden's compound did not have Internet access, but the Washington Times [reported](#) he had a "dedicated fiber-optic cable used for point-to-point access to the Internet," citing two U.S. officials who read after-action reports on the raid.)

A [job description](#) posted by MPRI, a division of defense contractor L-3, provides a few hints about what tools NMEC uses.

The NMEC support job, which requires a Top Secret security clearance, calls for "complete training in EnCase Forensic Software up through the EnCase Advanced training course or equivalent." A bachelor's degree in computer engineering is preferred. So is proficiency in "creating databases in MS Access and SQL."

Captured Al Qaeda computers have yielded useful intelligence before. A 2007 Defense Department "summary of evidence" supporting the charges against Khalid Sheikh Mohammed reported that a hard drive seized during his capture contained information on the four airplanes hijacked on 9/11, including code names, airline company, flight number, target, pilot name and background information, and names of the hijackers.

Also on the seized computer gear, the summary says: three letters from bin Laden, spreadsheets outlining financial assistance to families of known al Qaeda members, the "operational procedures and training requirements" for an al Qaeda cell, and transcripts of chat sessions belonging to one of the hijackers.

Bin Laden's Computers Will Test US Forensics

Ramzi Yousef, the original World Trade Center bomber, saved plans to bomb American jumbo jets flying over the Pacific on encrypted files on his laptop computer. (The FBI was able to bypass the encryption--Yousef apparently didn't use a high-security passphrase.)

But if whoever used the computer took the proper precautions, encryption could pose an obstacle, forensics specialists say. Well-designed encryption is now built into operating systems, including Apple's FileVault and Microsoft's BitLocker. PGP [announced](#) whole disk encryption for Windows in 2005; it's also [available](#) for OS X.

To avoid having to perform brute-force attacks to guess the passphrase, the Secret Service has found that it's better to seize a computer that's still turned on with the encrypted volume mounted and the encryption key and passphrase still in memory. "Traditional forensics always said pull the plug," U.S. Secret Service agent Stuart Van Buren [said](#) in February. "That's changing. Because of encryption...we need to make sure we do not power the system down before we know what's actually on it."

A team of researchers including Princeton University computer scientists [published a paper](#) in February 2008 that describes how to bypass encryption products by gaining access to the contents of a computer's RAM--through a mechanism as simple as booting a laptop over a network or from a USB drive--and then scanning for encryption keys.

U.S. law enforcement, at least, is now doing precisely that. "Our first step is grabbing the volatile memory," Van Buren said. One forensics utility the Secret Service has used is [Responder Pro](#), which allows the examination of volatile memory and is marketed as being able to unearth "chat sessions, registry keys, encryption keys, socket information and more."

Of course, not all useful information is digital. Yesterday's [warning](#) about train security from Homeland Security was triggered by files captured during the raid--not electronic ones: the source was "a set of handwritten notes," [according to](#) The Wall Street Journal.

Iran's Answer to Stuxnet

Iran's Answer to Stuxnet

Might a "halal Internet" be in the wings?

CYRUS FARIVAR 04/25/2011

Despite all of the talk that the Web fueled revolutions in Tunisia and Egypt, it remains clear that social media, or even increased Internet access, does not necessarily make revolution more likely. Even so, Iran would seem primed for an upheaval of the Islamic theocracy that has ruled the country since 1979. After all, Iran has one of the youngest, most educated and most wired populations in the Middle East. Some 70 percent of the country is under the age of 30, and the overwhelming majority of Iranians are literate. In fact, within the last several years, women have overtaken men in Iranian universities. Meanwhile, Iran's Internet penetration rate—the percentage of the population that is online—hovers around 35 percent, the highest percentage in the Middle East behind Israel. It made sense that the June 2009 uprising in Iran was thought to have been helped along by postings on Twitter, before it became more apparent that it wasn't significantly so.

The massive street protests in that uprising, which came in the wake of a disputed presidential election, were brought down with swift and brutal violence by the Revolutionary Guard and the Basij, Iran's vice police force. And besides such aggressive tactics offline, Iran is pursuing more and more sophisticated strategies online as well.

Two weeks ago, Ali Aghamohammadi, the Ahmadinejad Administration's head of economic affairs, was quoted in IRNA, a state-run news agency, that Iran was working on a "halal Internet."

"Iran will soon create an Internet that conforms to Islamic principles, to improve its communication and trade links with the world," he said, explaining that the new network would operate in parallel to the regular Internet and would possibly eventually

Iran's Answer to Stuxnet

replace the open Internet in Muslim countries in the region. "We can describe it as a genuinely 'halal' network aimed at Muslims on a ethical and moral level," he added.

It remains unclear exactly what a "halal Internet" would entail. Presumably, by definition, it would exclude the "haram Internet," (the Muslim equivalent of un-kosher)--so no pornography, for example. Likely, it would also feature the writings of revered Iranian Islamic leaders (the founder of the Islamic Republic, Ayatollah Khomeini, would be an obvious choice), as well as current Supreme Leader Ayatollah Khamenei, and other clerics who preach the gospel of the velayat-e faqih, the principle of the "rule of the [Islamic] jurist" that has governed Iran for three decades. But beyond religious scholarship, a halal Internet probably would also feature Iran's answer to Al Jazeera and the BBC--Press TV, which already has an English-language website.

It would be unlikely, but not technically impossible, for Iran to step up its censorship and filtering regime to create this "halal Internet." After all, most Cubans, for example, are priced out of the actual Internet and steered towards the Cuban equivalent, which is restricted to an internal e-mail network, and a handful of pro-government sites. In a similar vein, the Chinese Internet is limited largely only to websites that the government doesn't view as threatening.

This isn't the first time that the Islamic Republic has tried to co-opt the Internet for its own purposes. In fact, Iran has a 10-year history of pursuing aggressive tactics online.

As early as 2000, Iran tried to fool Iranians by creating the website Montazery.com, which was an attempt to divert traffic from Montazeri.com, the true website of an Iranian dissident ayatollah under house arrest who had written a scathing memoir against Khomeini and the Islamic Republic.

Over the next several years, Iran pursued a campaign of sophisticated filtering and censorship online, while also aggressively intimidating, arresting, and forcing into exile a number of young bloggers. By mid-decade, Iran was actively encouraging pro-

Iran's Answer to Stuxnet

regime bloggers, and said in 2008 that it would unleash an "army" of 10,000 bloggers from its own Revolutionary Guard.

In the months after the so-called "Twitter Revolution," the office of Supreme Leader Ayatollah Khamenei joined the micro-blogging service (@khamenei_ir), sending out 140 characters of propaganda—in English and Persian—at a time.

More recently, in fact, just before the Persian New Year, on March 20, 2011, a pro-regime blogger, Omid Hosseini, was proclaimed to be the winner of a government-sponsored blogging contest--only open to blogs that were not filtered in-country (meaning they are pro-regime), of course.

But there's likely a lot more to come out of the Iranian online world, particularly now that Iran has declared that it believes the United States and Israel were behind the creation of the infamous Stuxnet worm that likely set back Iran's nuclear program. (The New York Times had arrived at a similar conclusion months earlier.)

In an interview published in IRNA on April 16, Gholam Reza Jalali, the commander of the Iranian civil defense organization, was quoted as saying that Iran was creating the "1390 Program"—1390 being the current year in the Persian calendar—which would add six cyberdefense master's degree programs and one doctoral program across various Iranian universities.

"The final solution to problems of [cyberdefense and the] formation of Jihad, is to achieve economic self-sufficiency in the production of basic software such as operating systems and software," he said.

Cyrus Farivar (@cfarivar) is the author of The Internet of Elsewhere (Rutgers University Press, 2011), a book about the history and effects of the Internet in Senegal, South Korea, Estonia, and Iran.

Federal Radio Navigation Plan Relies on GPS, With No Backup

Federal radio navigation plan relies on GPS, with no backup

BY BOB BREWIN 04/22/2011

The federal government intends to rely on the Global Positioning System for precision navigation, location and timing services for the foreseeable future, with no defined backup, according to a key planning document released Thursday by the Defense, [Homeland Security](#) and Transportation departments.

The [2010 Federal Radio Navigation Plan](#) also envisions decommissioning key ground band navigation aids maintained by the Federal Aviation Administration as it moves to its GPS-based Next-Generation Air Transportation System.

Homeland Security approved the 219-page plan in March and Transportation last December. Defense Secretary Robert Gates signed it on April 15, three weeks after Deputy Secretary of Defense William J. Lynn III and Deputy Secretary of Transportation John Porcari blasted [plans](#) by startup cellular carrier LightSquared to operate in a frequency band that could interfere with GPS receivers.

Last November the National Space-Based Position, Navigation and Timing (PNT) Advisory Board, chaired by former Defense Secretary James Schlesinger, [warned](#) that the proliferation of inexpensive GPS [jammers](#) widely available for purchase over the Web made development of a backup system for GPS a national imperative.

Despite this warning and the potential of interference from LightSquared, the latest radio navigation plan did not identify a specific backup system for GPS. The plan said Homeland Security "is determining whether alternative backups or contingency plans exist." But, the plan added, "An initial survey of the federal critical infrastructure partners indicated wide variance in backup system requirements ... DHS is working with federal partners to clarify the operational requirements."

The PNT advisory board recommended using a system called eLORAN as a GPS backup, but President Obama zeroed out funding for LORAN (LONg RANGE Navigation) project in his 2010 budget, and the U.S. Coast Guard started shutting down the system and [blowing up](#) its towers last April.

The advisory board said FAA is exploring an alternative ground-based navigation system, but the earliest it would be capable of operation is 2025. In the meantime, FAA intends to divest to private operators or decommission ground-based navigation systems, the plan said. FAA operates 1,200 instrument landing systems to aid precision approaches, and the plan said FAA may shut some of these down, once GPS augmentation systems become operational. FAA has also targeted for

Federal Radio Navigation Plan Relies on GPS, With No Backup

eventual closure another 1,000 ground-based systems that provide heading information to pilots.

The plan also calls for Homeland Security to develop systems to mitigate the effect of jammers on GPS, but does not detail any specific systems.

This March the Royal Institute of Navigation in the United Kingdom released a [report](#) that warned that "Society may already be dangerously overreliant on satellite radio navigation systems like GPS ... The range of applications using the technology is now so broad that, without adequate independent backup, signal failure or interference could potentially affect safety systems and other critical parts of the economy."

David Last, a consultant to the General Lighthouse Authorities of the United Kingdom and Ireland, which operates aids to navigation systems in those countries, said, "It is difficult for international observers to see consistency in U.S. radio navigation policy."

While the PNT advisory board called for development of GPS backup systems, the radio navigation plan abandons that "in the hope that detection and mitigation of interference will save the day" Last said. He found it odd that the plan did not include any GPS backup, even as Defense and Transportation raised serious concerns about the potential of interference to GPS by LightSquared.

Really Remote Data

Really Remote Data

Far-flung data centers could use otherwise unharvestable renewable energy for computation.

By Christopher Mims

Researchers at Cambridge University want to put data centers in places so remote they aren't on any power grid. Their models indicate that moving data-hungry computation to places such as scorching deserts, windswept peaks, and the middle of the Atlantic Ocean—all rich in sunlight and wind energy—could allow this otherwise unharvestable energy to do useful work.

In a paper to be delivered at the 13th annual HotOS conference in May, the authors offer an extreme model of how cloud services could incorporate remote data centers powered only by renewable energy. Their scenario sites one solar- and wind-powered data center in the desert of southwest Australia and a second one in Egypt, on other side of the planet. This placement is no accident: putting them in different hemispheres, on opposite sides of the earth, maximizes the solar and wind energy they can harvest.

One catalyst for such a radical rethinking of how data centers can be sited and powered is the increasing availability of advanced fiber-optic networks. Connecting a remote renewable-energy plant to a power grid remains prohibitively expensive, reasoned the researchers working on this project—Sherif Akoush, Ripduman Sohan, Andrew Rice, Andrew W. Moore, and Andy Hopper—but running fiber-optic cable to such a plant would be relatively easy and cheap.

"We envisage data centers being put in places where renewable energy is being produced and you could never economically bring it back to heat a house," says Andy Hopper, senior author on the paper and head of Cambridge University's computer science department. "But you could lay a fiber and use energy that is otherwise lost, in that it's not economically transportable." One way to think of the underlying principle, he notes, is that it's easier to move bits (made up of photons) than electrons.

Jonathan Koomey, a researcher and consulting professor at Stanford, cautions that a number of real-world factors could render the Cambridge team's hypotheticals invalid. While data centers are costly, Koomey explains, the value they create is so far in excess of those costs that anything that reduces their effectiveness would reduce their net benefit to society.

Really Remote Data

"If the actions you take to save costs would also cut into the number of computations that you can then deliver, you'll reduce economic benefits from data centers, and that's presumably not what the authors had in mind," says Koomey.

Hopper, however, points out that the larger effort of which this paper is a part—the Computing for the Future of the Planet project—takes it as a given that more computing is always good, because the virtualization of goods and services displaces more energy-intensive activities in the physical world. He says that a system like the one he proposes would be implemented only at either "no cost to overall performance [of a cloud computing system] or at an attractive cost to performance."

The key to incorporating far-flung, intermittently available data centers into a cloud infrastructure, says Ripduman Sohan, a postdoctoral fellow who worked on the paper, is to be choosy about which processes are offloaded to them.

"I think Facebook would not want to put forward-facing Web services onto an architecture like this, for various reasons," says Sohan. However, a company like Facebook could offload projects that are not particularly time-sensitive but still sizable, such as processing analytics. "There are a bunch of batch-type jobs that could easily be offloaded to an architecture like this," says Sohan.

At least one real-world implementation of a system similar to the one proposed by the Cambridge team already exists. Called the GreenStar Network, it connects data centers powered entirely by renewable energy in Canada, Spain, Ireland, and Iceland. So far, the challenges inherent in porting large amounts of data and live computing processes from one data center to another in near-real time have been significant but surmountable.

The network uses supervisor software to shift computing according to the availability of wind and solar power at various sites, and, says Martin Brooks, an independent research consultant working on the GreenStar Network, this works well enough to allow the network to handle even finicky applications like running a video server. The video, says Brooks, doesn't skip even as the virtual machines hosting it are transferred, over an ultrafast fiber-optic network, between servers thousands of miles apart. "We have certainly had people consider [this project] outlandish, but we live it every day, so we don't think that way," he says.

Whether the Cambridge research will result in data centers in places as exotic as platforms in the middle of the Atlantic is anyone's guess, says Hopper, who also admits that some of his visions for the project may be over the top. His colleague Sohan is

Really Remote Data

less ambitious. "Sometimes when I talk to Hopper about this, I say that an easy way to bootstrap this project is to put a Sun modular data center in existing renewable energy sites."

Sun already has a data center that fits in a single shipping container, notes Hopper. Getting one to a renewable energy plant is as simple as taking it there on a truck. Connecting it to the Internet, however, is another matter: the team's models are based on the kind of high-speed fiber-optic networks that are available to academics but have yet to become economical for most commercial applications. Once they are, says Hopper, "we imagine putting photons into places that are godforsaken for every other reason except for generating energy."

Copyright Technology Review 2011.

Microsoft Business Suite Wins Federal Certification

Microsoft business suite wins federal certification

by Jay Greene

Microsoft's Business Productivity Online Services-Federal product [just won certification](#) from the federal government under the Federal Information Security Management Act, a bit of news that would have meant nothing to more than a handful of folks who follow the arcana of such things just a few weeks ago.

But earlier this month, Microsoft [called out rival Google](#) for allegedly misleading customers about the FISMA certification of its competing Google Apps for Government service. Microsoft's corporate vice president and deputy general counsel, David Howard, said that Google's Web-based productivity suite for government clients didn't have FISMA certification, even though Google had said it did.

Google [denied the charges](#), saying the technology platform of the product, Google Apps Premier Edition, is certified. According to Google, the government determined that the name change to Google Apps for Government, and increased security Google baked into that product, could be incorporated into the existing FISMA certification.

And Google went on to point out that, despite Microsoft's protestations, Business Productivity Online Services-Federal lacked its own FISMA certification. The backdrop for the battle is a lawsuit filed by Google over the Interior Department's decision to award Microsoft a contract to provide Web-based e-mail, business that Google would like for itself.

Microsoft's announcement that the Business Productivity Online Services-Federal received FISMA certification isn't likely to alter the landscape in the ongoing battle with Google. But the certification does open doors for Microsoft to win contracts with federal agencies, which make purchasing decisions, in part, based on the security accreditation.

The U.S. Department of Agriculture issued the certification and intends to migrate 120,000 employees to the Microsoft technology.

Carnegie Mellon Researchers Build Time Machine That Allows Visual Exploration of Space and Time

Carnegie Mellon Researchers Build Time Machine That Allows Visual Exploration of Space and Time

Time-lapse GigaPans Provide New Way To Access Big Data

Illah Nourbakhsh provides a guided tour of GigaPan Time Machine's feature.

PITTSBURGH—Researchers at Carnegie Mellon University's [Robotics Institute](#) have leveraged the latest browser technology to create [GigaPan Time Machine](#), a system that enables viewers to explore gigapixel-scale, high-resolution videos and image sequences by panning or zooming in and out of the images while simultaneously moving back and forth through time.

Viewers, for instance, can use the system to focus in on the details of a booth within a panorama of a carnival midway, but also reverse time to see how the booth was constructed. Or they can watch a group of plants sprout, grow and flower, shifting perspective to watch some plants move wildly as they grow while others get eaten by caterpillars. Or, they can view a computer simulation of the early universe, watching as gravity works across 600 million light-years to condense matter into filaments and finally into stars that can be seen by zooming in for a close up.

"With GigaPan Time Machine, you can simultaneously explore space and time at extremely high resolutions," said Illah Nourbakhsh, associate professor of robotics and head of the CREATE Lab. "Science has always been about narrowing your point of view — selecting a particular experiment or observation that you think might provide insight. But this system enables what we call exhaustive science, capturing huge amounts of data that can then be explored in amazing ways."

The system is an extension of the [GigaPan](#) technology developed by the [CREATE Lab](#) and NASA, which can capture a mosaic of hundreds or thousands of digital pictures and stitch those frames into a panorama that be interactively explored via computer. To extend GigaPan into the time dimension, image mosaics are repeatedly captured at set intervals, and then stitched across both space and time to create a video in which each frame can be hundreds of millions, or even billions of pixels.

An enabling technology for time-lapse GigaPans is a feature of the HTML5 language that has been incorporated into such browsers as Google's Chrome

Carnegie Mellon Researchers Build Time Machine That Allows Visual Exploration of Space and Time

and Apple's Safari. HTML5, the latest revision of the HyperText Markup Language (HTML) standard that is at the core of the Internet, makes browsers capable of presenting video content without use of plug-ins such as Adobe Flash or Quicktime.

Using HTML5, CREATE Lab computer scientists Randy Sargent, Chris Bartley and Paul Dille developed algorithms and software architecture that make it possible to shift seamlessly from one video portion to another as viewers zoom in and out of Time Machine imagery. To keep bandwidth manageable, the GigaPan site streams only those video fragments that pertain to the segment and/or time frame being viewed.

"We were crashing the browsers early on," Sargent recalled. "We're really pushing the browser technology to the limits."

Guidelines on how individuals can capture time-lapse images using GigaPan cameras are included on the site created for hosting the new imagery's large data files, <http://timemachine.gigapan.org>. Sargent explained the CREATE Lab is eager to work with people who want to capture Time Machine imagery with GigaPan, or use the visualization technology for other applications.

Once a Time Machine GigaPan has been created, viewers can annotate and save their explorations of it in the form of video "Time Warps."

Though the time-lapse mode is an extension of the original GigaPan concept, scientists already are applying the visualization techniques to other types of Big Data. Carnegie Mellon's [Bruce and Astrid McWilliams Center for Cosmology](#), for instance, has used it to visualize a simulation of the early universe performed at the Pittsburgh Supercomputing Center by Tiziana Di Matteo, associate professor of physics.

"Simulations are a huge bunch of numbers, ugly numbers," Di Matteo said. "Visualizing even a portion of a simulation requires a huge amount of computing itself." Visualization of these large data sets is crucial to the science, however. "Discoveries often come from just looking at it," she explained.

Rupert Croft, associate professor of physics, said cosmological simulations are so massive that only a segment can be visualized at a time using usual techniques. Yet whatever is happening within that segment is being affected

Carnegie Mellon Researchers Build Time Machine That Allows Visual Exploration of Space and Time

by forces elsewhere in the simulation that cannot be readily accessed. By converting the entire simulation into a time-lapse GigaPan, however, Croft and his Ph.D. student, Yu Feng, were able to create an image that provided both the big picture of what was happening in the early universe and the ability to look in detail at any region of interest.

Using a conventional GigaPan camera, Janet Steven, an assistant professor of biology at Sweet Briar College in Virginia, has created time-lapse imagery of rapid-growing brassicas, known as Wisconsin Fast Plants. "This is such an incredible tool for plant biology," she said. "It gives you the advantage of observing individual plants, groups of plants and parts of plants, all at once."

Steven, who has received GigaPan training through the [Fine Outreach for Science program](#), said time-lapse photography has long been used in biology, but the GigaPan technology makes it possible to observe a number of plants in detail without having separate cameras for each plant. Even as one plant is studied in detail, it's possible to also see what neighboring plants are doing and how that might affect the subject plant, she added.

Steven said creating time-lapse GigaPans of entire landscapes could be a powerful tool for studying seasonal change in plants and ecosystems, an area of increasing interest for understanding climate change. Time-lapse GigaPan imagery of biological experiments also could be an educational tool, allowing students to make independent observations and develop their own hypotheses.

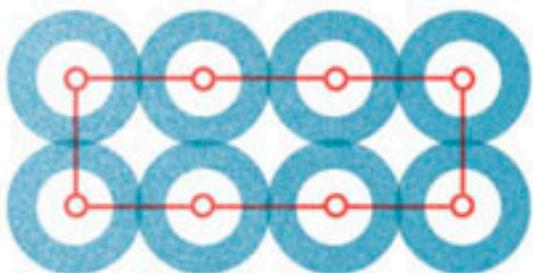
Google Inc. supported development of GigaPan Time Machine.

Chinese Chips Wins Energy Efficiency Crown

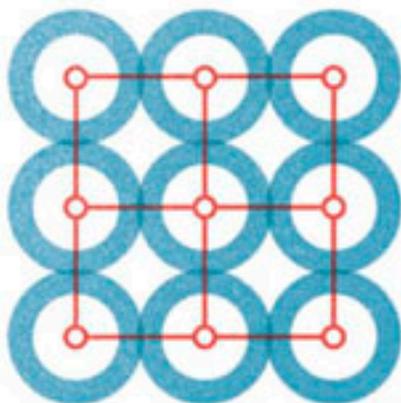
Chinese Chip Wins Energy-Efficiency Crown

Though slower than competitors, the energy-saving Godson-3B is destined for the next Chinese supercomputer

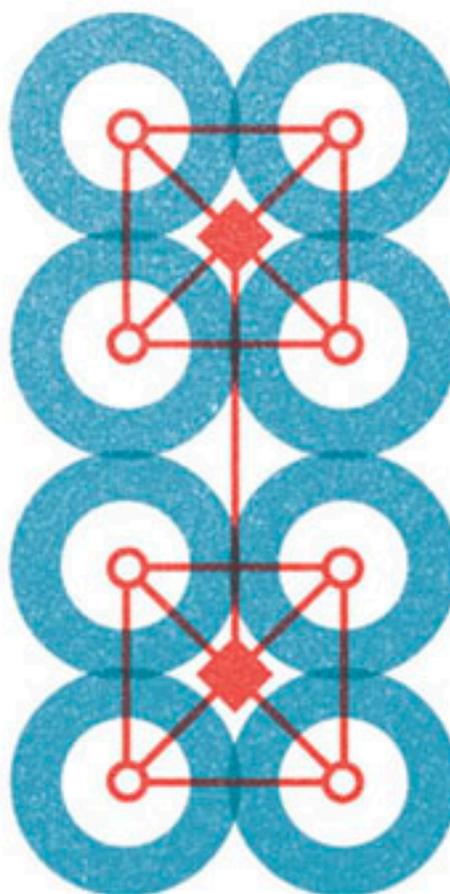
By JOSEPH CALAMIA / MAY 2011



8-CORE RING: In most microprocessors, information circles around a ring-shaped interconnect to reach processor cores.



9-CORE MESH: Some new high-end processors use a mesh network. These can be more complex but also more energy efficient.



8-CORE GODSON: The Chinese processor relies on a modified mesh network that contains extra direct connections to move data efficiently.

ILLUSTRATIONS: GAVIN POTENZA

Chinese Chips Wins Energy Efficiency Crown

The Dawning 6000 supercomputer, which Chinese researchers expect to unveil in the third quarter of 2011, will have something quite different under its hood. Unlike its forerunners, which employed American-born chips, this machine will harness the country's homegrown high-end processor, the Godson-3B. With a peak frequency of 1.05 gigahertz, the Godson is slower than its competitors' wares, at least one of which operates at more than 5 GHz, but the chip still turns heads with its record-breaking energy efficiency. It can execute 128 billion floating-point operations per second using just 40 watts—double or more the performance per watt of competitors.

The Godson has an eccentric interconnect structure—for relaying messages among multiple processor cores—that also garners attention. While Intel and IBM are commercializing chips that will shuttle communications between cores merry-go-round style on a "ring interconnect," the Godson connects cores using a modified version of the gridlike interconnect system called a mesh network. The processor's designers, led by Weiwu Hu at the Chinese Academy of Sciences, in Beijing, seem to be placing their bets on a new kind of layout for future high-end computer processors.

A mesh design goes hand in hand with saving energy, says Matthew Mattina, chief architect at the San Jose, Calif.–based Tilera Corp., a chipmaker now shipping 36- and 64-core processors using on-chip mesh interconnects.

Imagine a ring interconnect as a traffic roundabout. Getting to some exits requires you to drive nearly around the entire circle. Traveling away from your destination before getting there, says Mattina, requires more transistor switching and therefore consumes more energy. A mesh network is more like a city's crisscrossed streets. "In a mesh, you always traverse the minimum amount of wire—you're never going the wrong way," he says.

On the 8-core Godson chip, 4 cores form a tightly bound unit—each core sits on a corner of a square of interconnects, as in a usual mesh. Godson researchers have also connected each corner to its opposite, using a pair of diagonal interconnects to form an X through the square's center. A "crossbar" interconnect then serves as an overpass, linking this 4-core neighborhood to a similar 4-core setup nearby.

Chinese Chips Wins Energy Efficiency Crown

Godson developers believe that their modified mesh's scalability will prove a key advantage, as chip designers cram more cores onto future chips. Yunji Chen, a Godson architect, says that competitors' ring interconnects may have trouble squeezing in more than 32 cores.

Indeed, one of the ring's benefits could prove its future liability. Linking new cores to a ring is fairly easy, says K.C. Smith, an emeritus professor of electrical and computer engineering at the University of Toronto. After all, there's only one path to send information—or two in a bidirectional ring. But sharing a common communication path also means that each additional core adds to the length of wire that messages must travel and increases the demand for that path. With a large number of cores, "the timing around this ring just gets out of hand," Smith says. "You can't get service when you need it."

Of course, adding more cores in a mesh also stresses the system. Even if you have a grid of paths providing multiple communication channels, more cores increase the demand for the network, and more demand makes traveling long distances difficult: Try driving across New York City at rush hour. Still, the bandwidth scaling of a mesh interconnect is superior to that of a ring, Tlera's Mattina says. He notes that the total bandwidth available with a mesh interconnect increases as you add cores, but with a ring interconnect, the total bandwidth remains constant even as the core count increases. Latency—the time it takes to get a message from one core to another—is also more favorable in a mesh design, Chen says. In a ring interconnect, latency increases linearly with the core count, he says, while in a mesh design it increases with the square root of the number of cores.

Reid Riedlinger, a principal engineer at Intel, points out that a ring interconnect has its own scalability benefits. Intel's recently unveiled 8-core Poulson design employs a ring not only to add more cores but also to add easy-to-access on-chip memory, or cache. As long as the chip has the power and the space, Riedlinger says, a ring makes it easy to add each core and cache as a module—a move that would require more complicated validity studies and logic modification in a mesh. "Adding the additional ring stop has a very small impact on latency, and the additional cache capacity will provide performance benefits for many applications," he says.

Chinese Chips Wins Energy Efficiency Crown

For those who are not building a national supercomputer, Riedlinger also points out that a ring setup is more easily scalable in a different direction. "You might start with an 8-core design," he says, "and then, to suit a different market segment, you might chop 4 cores out of the middle and sell it as a different product."

This article originally appeared in print as "China's Godson Gamble".

Translating the Web While You Learn

Translating the Web While You Learn

A new website will offer free language lessons—and use the results to render Web pages in other tongues.

By Christopher Mims

The creators of a website called **Duolingo** want to translate the world's Web pages into new languages by harnessing the efforts of people who are learning those languages.

If the approach sounds familiar, it's because a similar idea is the basis of the effort known as **reCAPTCHA**, which was invented by the same Carnegie Mellon computer science professor behind the new project: Luis von Ahn.

A recaptcha is a string of distorted text shown to a user trying to register for a new account or comment on a Web page; the text comes from electronically scanned print that could not be recognized by a computer. To gain permission, the user must reënter the words correctly. More than a hundred million recaptchas are solved each day. Von Ahn says that if he can capture even a small portion of that audience with Duolingo—say, a million users—he could translate all of Wikipedia's English entries into Spanish in 80 hours.

Even though the Duolingo site has yet to launch—von Ahn says it will enter private beta "on the order of weeks" from now—he was able to reveal a few details about how it operates. The basic premise is simple: users, even those who have never spoken a particular language before, are presented with short phrases on which to practice. The system helps them by defining some of the words in the phrase.

Users' attempts to translate the phrase are later voted on by other users, and the most accurate translation "wins." In a talk given at a recent TEDx conference at Carnegie Mellon, he said that the results "are as accurate as translations from professional language translators."

As for Duolingo's capabilities as a language teacher, Von Ahn says his team's tests indicate that users "do about as well as with other methods."

Duolingo has one big advantage over other language tools: it's free. This means its potential audience is enormous, encompassing anyone with a computer. Eventually, says von Ahn, he wants to make the system accessible by mobile phones, which would increase its reach by hundreds of millions, if not billions, of potential users.

Translating the Web While You Learn

"These guys are brilliant," says Christopher O'Donnell, former head of product at Transparent, a maker of language-learning software whose customers include the U.S. Department of Defense. "They might be on to something super elegant and amazingly perfect, like recaptcha was. If they do the recaptcha of language, it's massive."

But Duolingo's success will depend in no small part on whether the site can keep users coming back. To that end, the system has been tested and updated continually since the fall of 2010.

"A huge part [of making it successful] is that you just need to experiment. It's nothing but trial and error," says Severin Hacker, a PhD student at Carnegie Mellon and the lead architect of Duolingo.

Initially, Duolingo will launch with just three languages: English, Spanish, and German. The eight-member team working on the project had originally intended to tackle more, but they soon discovered that development time was too slow for languages that were not native to at least one team member.

Severin says the multilingual nature of Duolingo was one of the biggest challenges in its development. Users with keyboard layouts intended for English, for example, cannot easily generate special characters used in other languages, such as the umlaut in German. As a result, developers and the team's designer had to put a lot of effort into honing the interface, including developing a fast and intuitive virtual keyboard for generating these characters.

Aside from the promise of free language instruction, it isn't clear how Duolingo may entice users. But many of von Ahn's past projects have involved casual games designed to encourage them to perform useful tasks that computers can't manage on their own. (One game he developed, which makes it fun for users to label images, was later purchased by Google and now enhances the utility of Google Image Search.)

"A hard thing when learning a language is just staying motivated," says von Ahn. "A large fraction of people want to learn a language, but at end of day it is hard to do it. We had to tackle that problem."

Another hurdle to the success of Duolingo is that unlike recaptcha, which is embedded on countless websites, Duolingo will require that users show up in the first place. Von Ahn says he has no idea whether it will generate sufficient attention, but interest is already high. So many people have already signed up for the private beta, he says,

Translating the Web While You Learn

that "if we only had those users, we could already translate a lot of stuff."

Copyright Technology Review 2011.

Targeting Left Over Land Mines

Targeting leftover land mines

New smartphone-aided technology makes dangerous task easier

By Rebecca Hersher '11

Harvard Correspondent

Wednesday, May 4, 2011



Justin Ide/Harvard Staff Photographer

Lahiru Jayatilaka (above) and Krzysztof Gajos at the Harvard School of Engineering and Applied Sciences have helped develop a new and improved means of finding and removing land mines from current and former war zones. The new system uses smartphones with the conventional metal detectors to help de-miners better visualize what they are detecting.

L

and mines remain among the most destructive remnants of 20th century warfare, continuing to slow resettlement and hinder recovery in many former war zones.

While mine-clearing protocols have improved substantially since World War II, the technology used to locate buried landmines has changed little: De-miners use metal detectors to find and identify mines. On a battlefield strewn with metal debris, differentiating lethal mines from benign cans, wires, and casings is enormously time consuming.

Now, computer scientists at the [Harvard School of Engineering and Applied Sciences](#) (SEAS) have designed an elegant system that ties in smartphones to assist humanitarian de-miners by augmenting the information supplied by their metal

Targeting Left Over Land Mines

detectors. Their system, known as pattern enhancement tool for assisting land mine sensing ([PETALS](#)), and which will be presented at this week's Conference on Human Factors in Computing Systems, takes de-mining advances in a new direction.

“We want to support people in the field with minimal invasiveness. Without changing their sweeping style, without giving them new procedures, this technology allows them to better visualize what they are detecting,” explained SEAS researcher [Lahiru Jayatilaka](#), who is working with Assistant Professor of Computer Science [Krzysztof Gajos](#) at SEAS, James Staszewski of [Carnegie Mellon University](#), and Luca Bertuccelli of [Massachusetts Institute of Technology](#).

In the field, de-miners use a repetitive sweeping motion to systematically cover small sections of ground looking for land mines. When the metal detector passes over a metallic object, it beeps. Expert de-miners are able to visualize the auditory feedback of the metal detector, creating in their heads an image of the object's outline underground. Land mines, with their circular construction and trigger pin, have an ovoid signature. The system designed by Jayatilaka and Gajos shows one red dot for every beep of the metal detector. With passes over a buried object, the picture shows an increasingly complete outline of the object's shape, giving the de-miner an evermore detailed picture of what may be buried there.

“Using only audio signals is a huge source of inefficiency. The operator has to figure out whether it is harmful or not harmful. If they are not completely sure, they have to go down on their hands and knees and excavate every piece of metal as if it were a land mine,” explained Jayatilaka.

Most humanitarian de-mining programs operate in developing countries where resources are highly constrained. Among the challenges Jayatilaka and Gajos faced was designing an affordable system requiring minimal field maintenance. Their solution

Targeting Left Over Land Mines

involved a cheap and ubiquitous platform: the smartphone. The final version of PETALS is designed to run on a normal mobile device such as an iPhone, which can be mounted on a metal detector.

In addition to increasing search efficiency, PETALS has the potential to help train new de-miners. In initial tests, novice de-miners performed 80 percent better with visual aid. Furthermore, Jayatilaka pointed out, training with a visual aid can help novices understand the principles of recognizing land mine signatures more quickly, allowing them to gain more from training.

“Improving the de-miner rather than the equipment is a novel way to think about land mine removal technology,” said Jayatilaka. “It is a new direction for the field.”

BAMS Program Office Seeks to Integrate Air Force SIGINT Sensor Into Platform

BAMS Program Office Seeks To Integrate Air Force SIGINT Sensor Into Platform
(DEFENSE DAILY 20 APR 11) ... Carlo Munoz

The Navy program office in charge of the service's newest unmanned aerial system is looking to integrate Air Force-centric hardware into that aircraft, as a way to close a critical collection gap in ongoing intelligence, surveillance and reconnaissance operations.

Members of the Navy's Persistent Maritime Unmanned Aircraft Systems program office (PMA-262) are exploring the integration of the Airborne Signals Intelligence Payload (ASIP) system currently on board the Air Force's RQ-4 Global Hawk unmanned aircraft into the Navy's Broad Area Maritime Surveillance (BAMS) UAS, program manager Capt. Bob Dishman said.

Both the BAMS and Global Hawk UAS are built by prime contractor Northrop Grumman [NOC].

The installation of the ASIP sensor platform would be one way Navy officials could meet key program requirements for future iterations of the BAMS aircraft, Dishman said.

The capability development document for the initial increment of the Navy's unmanned aerial system noted that future iterations of the aircraft would feature more robust communications relays and a signals intelligence capability, according to Dishman.

"Realize that the initial increment of BAMS does...cover a certain amount of the frequency spectrum with electronic support measures," he said. "What we do not have is the communications intelligence piece, so we would [have to] add that functionality to the airplane."

As part of that work, program officials are looking at the payload capacity and power currently on board the BAMS aircraft, and what modifications would be needed to get that additional communications and SIGINT into the platform.

"We are working with [N2/N6] staff to further define what kind of SIGINT capability [they] would like to have on BAMS." The N2/N6 is the Navy's Information Dominance directorate, which handles ISR requirements and capabilities for the sea service.

One of the advantages of integrating the ASIP into the Navy UAS is that it would build upon the growing Navy-Air Force cooperation on this program. Although the two platforms are designed to meet service-specific requirements, similarities in the airframes and functionality warrant a joint effort to achieve maximum efficiency, service officials have said in the past (Defense Daily, July 2, 2010).

The air service "could probably have a lot of synergy with the Navy if we just adopt the Air Force ASIP payload to meet our SIGINT capability," Dishman said. "So we are looking at that and [asking] does that make sense or are there other alternatives that meet the maritime frequencies that we are looking for."

Along with looking at mounting an ASIP sensor into the aircraft's internal bays, Dishman said that an ASIP payload could also be mounted on an external pylon under one of the wings.

"We do have a couple of...points on the wing where we could provide electricity [and] could house some of the SIGINT," he said. Mounting an ASIP platform on a pylon "would be ideal" because then the unmanned aircraft would still be able to field its original sensor platform, housed

BAMS Program Office Seeks to Integrate Air Force SIGINT Sensor Into Platform

internally on board.

Whether Navy ISR officials opt to fill their SIGINT requirement with the ASIP or not, integrating a signals intel capability into BAMS will be the first step toward developing a "family of systems" to replace the Navy's legacy EP-3 spyplane.

This "family of systems approach" for fielding an EP-3 replacement will center around BAMS, as well as the Medium-Range UAS, which is still under development by the sea service, Vice Adm. David Dorsett, deputy chief of naval operations for information dominance and director of naval intelligence, said during a Jan. 5 Defense Writers Group breakfast in Washington.

Currently, Dishman's office is participating in the Navy's continuing work on the analysis of alternatives for the now-defunct EP-3 replacement program, tailoring that work to focus more on the family of systems concept now being followed by the Navy.

The Navy had been eyeing potential replacement options for the EP-3 since 2009, beginning with an Analysis of Alternatives (AoA) issued that year. However, the White House nixed the entire effort, known as EP-X, in its fiscal year 2011 defense budget proposal.

"I think there are some additional excursions that are going to happen with that AoA, [and] what we are doing now is looking at what capabilities could be out there," Dishman said.

Do Drones Make War Too Easy?

Do drones make war too easy?

By [Philip Ewing](#) Monday, April 25th, 2011 11:15 am

Via [Abu Muqawama](#), here's a question that WaPo's [Walter Pincus asked on Sunday](#): Do unmanned systems — in particular armed UAVs — make it too easy for top leaders to resort to violence? As Buzz readers know, the military has been using unmanned systems of various kinds for decades, but the UAV really came into its own over Iraq, Afghanistan and Pakistan, where local commanders cannot get enough of the high quality surveillance they provide. Of course, UAVs also enable senior leaders to do more than spy: They give the ability to attack targets without risking the life of a human pilot.

Pincus asks and answers some science fiction-style questions about whether drones will ever decide to attack targets on their own, but that's not in the cards for now. Still, the fundamental question is the most interesting: When the cost of military action does not involve risking American lives, does it make a president or a general that much likelier to use it? And do the same ethical and practical lines of thought apply across unmanned systems no matter what, or as ground and water drones become more advanced, will they require their own unique principles?

Quick thought experiment: Let's say the Army developed a big ground robot along the lines of Boston Dynamics' [Big Dog](#), with all the kinks worked out, with ideal sensors, realtime positive control, and onboard weapons. (Let's say a few guns and something like a 25mm grenade launcher.) We have no problem with a UAV orbiting overhead and firing a missile at a hut where suspected bad guys are hiding, but what about releasing a pack of Attack Dogs (as we'll call them) into the ungoverned tribal regions of Pakistan? Would it be acceptable for the pack to assault a suspected terrorist village on the ground because commanders believe that's where a high-value target is hiding? Advocates might argue the dogs could go in, positively ID individual terrorists and minimize the potential for the unintended casualties you can get in a strike from the air. They could also collect intelligence, of a sort, rather than just destroying all the documents and computers on hand as an air strike would.

Do those unmanned ground vehicles constitute a foreign invasion? Is shooting a man with a gun on a robot at close range different from blowing him up with a missile fired from a robot high above? (Let's pretend that every Attack Dog is controlled by a human operator, basically playing a first-person shooter video game that controls the real-life drone on the ground.) Now suppose the Army had a company of these Attack Dogs at about the same time as the White House was developing its plans to intervene in Libya. Would the president and the Pentagon be as reluctant to get involved on the ground if it meant sending unmanned systems against Qaddafi's troops, as opposed to

Do Drones Make War Too Easy?

human soldiers?

It all sounds pretty fanciful today, but it might not be long before presidents, Pentagon planners and lawmakers need to wrestle with such questions. What do you think? Could a new generation of advanced remotely operated weapons make the risks of war so low it becomes too easy to start one?

X-47B First Flight Hints At New Capabilities For Navy Carriers

X-47B First Flight Hints At New Capabilities For Navy Carriers
(*COMBAT AIRCRAFT MAGAZINE 30 APR 11*) ... David Axe

It was an event a century in the making. At 2:09 PM Pacific Standard Time on Feb. 4, the first full-scale prototype of Northrop Grumman's X-47B carrier-capable drone fighter took off on from Edwards Air Force Base in California for its inaugural test flight.

"Taking off under hazy skies, the X-47B climbed to an altitude of 5,000 feet, flew several racetrack-type patterns, and landed safely at 2:38 PM PST," Northrop announced in a press release. "The flight provided test data to verify and validate system software for guidance and navigation, and the aerodynamic control of the tailless design."

The X-47's first flight took place almost exactly 100 years after history's very first deck trap. On Jan. 18, 1911, American barnstorming pilot Eugene Ely landed his pusher biplane on a temporary deck fitted to the battleship USS Pennsylvania. The X-47's first flight was perhaps not as revolutionary as Ely's daring feat. But it did mark a potential huge leap in naval aviation development. With the X-47, Northrop "added just three words" to NAVAIR's traditional repertoire," said Navy Capt. Jamie Engdahl, program manager for the diamond-shaped, 62-foot-wingspan drone. Those three words are "unmanned, autonomous and L.O. relevant." "L.O." meaning "low-observable," or stealthy.

The X-47 or a follow-on design could radically improve the strike capabilities of today's short-range carrier air wings, while for the first time also allowing the Navy to conduct long-endurance armed surveillance, similar to what the Air Force does with its Predator and Reaper drones. The X-47 might also funnel technologies and ideas into a just-initiated effort to field a new heavy bomber for the Air Force.

The Unmanned Combat Air System-Demonstration program should culminate in carrier tests and in-air refueling of the X-47B drone no later than 2013. UCAS-D will transition into a more lucrative program called Unmanned Carrier-Launched Surveillance System, meant to field operational drones — either X-47s or a similar design — to carrier wings by 2018. Confidence in the two programs is so high that, weeks before the X-47's first flight, Secretary of Defense Robert Gates recommended adding funds to accelerate them.

It's not hard to see why Gates is so eager to deploy armed drones aboard carriers. In 2007, the influential Washington, D.C. think tank Center for Strategic and Budgetary Assessments examined the benefits of a carrier wing that adds a squadron of drones to its usual complement of around 40 F/A-18 strike fighters.

"Using manned aircraft, current CVWs are optimized to strike targets at ranges between 200 to 450 nautical miles from their carriers," CSBA's report asserted. "Moreover, carrier aircraft lack persistence. ... In contrast, a carrier-based UCAS could mount strikes out to 1,500 [nautical miles] from a carrier without refueling. Just as importantly, because its mission duration is not limited by human endurance, with aerial refueling a UCAS will be able to stay airborne for 50 to 100 hours — five to ten times longer than a manned aircraft."

"The strategic value of that sort of responsiveness and reach would be incalculable," CSBA

X-47B First Flight Hints At New Capabilities For Navy Carriers

concluded, without mentioning that the X-47 and similar drones would also be stealthier than an F-18.

An operational drone based on the X-47 is still seven years in the future, but it's possible the X-47 has already inspired the basic planform of a traditionally-piloted warplane. In February, the Pentagon announced a new program to build a fleet of up to 100 new, manned, stealth bombers for the Air Force, with the first combat squadron equipped sometime in the early 2020s.

The so-called "Long-Range Strike" design will likely remain cloaked in secrecy, and might not be competed, the military said. Indeed, according to some reports, a Northrop-built prototype is already flying. Several years ago, during an earlier, aborted attempt to build a new bomber, Northrop's own marketing department released artwork showing a large, manned strike plane with the same basic shape as the UCAS-D drone.

A hundred years after naval aviation's birth, the future of long-range strike for the Navy – and maybe the Air Force — is diamond-shaped, robotic and called "X-47."

Boeing Phantom Ray UCAS Makes First Flight

Boeing Phantom Ray UCAS Makes First Flight

POSTED BY: EVAN ACKERMAN / WED, MAY 04, 2011



It was barely two months ago that Northrop Grumman's X-47B Unmanned Combat Air System (UCAS) made its first autonomous flight. On April 27, Boeing's Phantom Ray followed suit on *its* first flight, maneuvering at 7,500 feet at speeds of over 175 knots. The test flight, which lasted just under 20 minutes, was followed by a perfect autonomous landing.

Obviously, this is just the first little taste of what the Phantom Ray is capable of. Its operational top speed is about 0.85 Mach, with a range of nearly 2,500 km. Further testing will explore the capabilities of the UCAS for "supporting missions that may include intelligence, surveillance, and reconnaissance; suppression of enemy air defenses; electronic attack; hunter/killer; and autonomous aerial refueling."

Boeing Phantom Ray UCAS Makes First Flight



It's worth mentioning that unlike the Northrop Grumman X-47B, the Phantom Ray is entirely Boeing's project. Northrop Grumman won DARPA's UCAS program, and the X-47B is being developed specifically for the US Navy. Even though Boeing's X-45 didn't get selected, Boeing decided not to just let the X-45 die off, and so they adapted it into the Phantom Ray instead. Just what exactly is going to happen to the program is anyone's guess; the possibilities range from keeping it as a testbed to turning it into a production prototype that's ready for deployment. And you know what *that* would mean... Sometime, somewhere, someone is going to get an X-47B and a Phantom Ray in the same piece of sky and just let them go at it, *Top Gun* style.

Boeing Phantom Ray UCAS Makes First Flight



Future UAVs Must Be Hardened

Future UAVs Must Be Hardened: USAF Officers

By DAVE MAJUMDAR

Published: 20 Apr 2011 18:52

Future unmanned aircraft will have to be designed to fly over hostile areas where an enemy would actively challenge their presence, a panel of three U.S. Air Force officers said.

While today's unmanned aircraft, such as the MQ-1 Predator and MQ-9 Reaper, fly over the uncontested skies of Iraq, Afghanistan or even Libya, tomorrow's wars may see a hostile power jam vulnerable data-links and global positioning system (GPS) signals while sending up fighters to force such planes out of their airspace, the men told an audience at a International Institute of Strategic Studies conference on April 20.

"We must continue to develop systems that are hardened against GPS-denied environments, hardened against comm-out environments, and partially hardened against aerial threats and ground threats," said Air Force Col. Dean Bushey, deputy director of the U.S. Army Joint Unmanned Aircraft Systems Center of Excellence.

Nor can the Air Force take the air bases it operates UAVs out of for granted, he added.

Such bases might come under attack from enemy forces, which would necessitate developing unmanned jets with greater range and persistence to enable such aircraft to operate from outside the range of those potential threats, said Mark Gunzinger, an analyst at the Center for Strategic and Budgetary Assessments in Washington.

However, communications could be the deciding factor for future unmanned aircraft.

"Stealth technology is such today that we can make platforms that are much, much more survivable," he said. "But controlling them is going to be a significant problem."

In fact, it might be that for operations inside defended airspace, manned aircraft would be the preferred option until a solution is found, Gunzinger said.

Future UAVs Must Be Hardened

One option is for an aircraft to be preprogrammed with a set route to attack a particular set of targets.

"But you'd be limited in your ability to deal with unplanned circumstances," Gunzinger said. Moving targets would be especially problematic because there would be no way to update the aircraft's target set en route.

Another alternative, Bushey suggested, might be to have the unmanned aircraft act as a "loyal wingman," where it would be led into combat by a manned aircraft.

Gunzinger agreed that the concept might be possible.

"That could be a feasible operational concept where one mother ship would control a number of unmanned platforms, not just for [Intelligence, Surveillance, Reconnaissance], but for a range of operations," he said.

Ideally, however, unmanned aircraft would be able to perform missions autonomously inside contested airspace.

Autonomy is necessary because an enemy would almost certainly attack the aircraft's vulnerable communications links, Gunzinger said. However, in any sort of threat environment, an unmanned aircraft would have to have the sensors to detect and avoid incoming threats, he added.

Bushey also emphasized a need for greater autonomy for unmanned aircraft.

However, autonomous aircraft that could independently perform such missions are not currently technologically feasible. Machines are not yet able to automatically recognize targets, nor are machines able to make decisions in a "dynamic" environment, such as air-to-air combat, said Col. James Sculerati, U.S. Special Operations Command's ISR chief. However, many routine tasks such as takeoffs and landings could be automated, Sculerati said.

Future UAVs Must Be Hardened

To build a truly autonomous aircraft would require computing power approaching genuine artificial intelligence, Gunzinger said.

"I don't think we're at a point where we're willing to have systems autonomously engage another system, but we can get to a point where we can have a system get there and then have human control," Bushey added.

Nearly a Decade Behind Schedule, New Satellite Is to Provide Earlier Missile-launch Warning

Nearly a decade behind schedule, new satellite is to provide earlier missile-launch

warning

BY WILLIAM MATTHEWS 04/26/2011

Nine years late, the Air Force is finally ready to launch a new missile-spotting satellite that it says will usher in "a new era in persistent infrared surveillance."

Barring further delays, the first of four Space-Based Infrared System satellites will blast off May 6 and climb to an altitude of about 22,200 miles, where it will park in a geosynchronous orbit and stare at Earth, watching for missile launches and searching for new military targets.

Air Force Brig. Gen. Roger Teague, chief of the Air Force Infrared Space Systems Directorate, emphasized the new satellite's expected capability during a telephone press conference Tuesday.

Infrared sensors on the spacecraft are "so much more sensitive" than those in use on current missile-detecting satellites, he said. "They can see much more much earlier" and they "can see much dimmer targets."

Teague said he could not elaborate on what more the sensors can see or what dimmer targets might be without disclosing classified information. Dimmer targets are expected to include smaller, shorter-range missiles.

While extolling the new satellite, Teague also acknowledged that the SBIRS program "has faced and overcome a number of challenges in the past."

Those include major delays and exorbitant costs. Begun in 1995, SBIRS was supposed to be a \$4.5 billion program that put new missile launch detecting satellites in orbit starting in 2002. Nearly a decade behind schedule, the program has consumed \$15.9 billion, and according to the Government Accountability Office, costs are still going up.

Teague said the last of four geosynchronous satellites now planned won't be launched until 2016 if the current schedule holds.

The SBIRS satellite constellation also includes four sensor payloads that are hosted on non-Air Force satellites in highly elliptical orbits, he said. Two of those already have been launched.

As they are launched one by one, the SBIRS satellites will begin augmenting the existing Defense Support Program system of early warning satellites that watch for hostile missile launches, Teague

Nearly a Decade Behind Schedule, New Satellite Is to Provide Earlier Missile-launch Warning

said. They will become "the gold standard for missile warning," he said.

In addition to missile launch warnings, the new satellites are intended to contribute to missile defense, to battle space awareness and to gather "technical intelligence," the Air Force says.

Their contribution to missile defense is to gather intelligence and send it to the ground to be processed and distributed fast enough to provide theater commanders with actionable intelligence for planning defenses, Teague said.

Gathering technical intelligence involves spotting new targets on the ground and gathering data "to figure out the profiles of the new targets," said Jeff Smith, a Lockheed Martin vice president for SBIRS.

Smith, too, noted the "many challenges" that SBIRS has faced, but said Lockheed is confident that the satellites "will meet or exceed customer expectations" to deliver "unprecedented global persistent and taskable infrared surveillance."

But even now, costs continue to escalate and there is danger of further delays, GAO told Congress in March. The Defense Contract Management Agency "projects nearly \$600 million in cost overruns at contract completion, more than twice the amount reported last year," GAO reported.

The SBIRS program office "is working to rebaseline" SBIRS cost and schedule estimates "for the sixth time," GAO said, referring to the process of re-estimating costs and schedules after they have been exceeded.

Recent delays were caused by faulty flight software designed to monitor the health of the satellite, GAO said.

Air Force's First Dedicated SBIRS Satellite Carried to Orbit

Air Force's First Dedicated SBIRS Satellite Carried to Orbit

By **Turner Brinton**



A United Launch Alliance (ULA) Atlas 5 launches the first dedicated SBIRS satellite. Credit: ULA photo

WASHINGTON — The U.S. Air Force successfully launched its first Space Based Infrared System (SBIRS) geosynchronous missile warning satellite May 7 aboard an Atlas 5 rocket from Cape Canaveral Air Force Station, Fla., the service announced May 7.

After nearly a decade of delay due to myriad technical and programmatic troubles, the first SBIRS satellite is expected to reach its final orbit in nine days. It will join the service's legacy Defense Support Program satellites on orbit to provide the United States with global, persistent surveillance of missile launches, as well as contributing to other missions such as missile defense and tactical intelligence.

The satellite was built by Lockheed Martin Space Systems of Sunnyvale, Calif., and the payload was developed by Northrop Grumman Electronic Systems of Azusa, Calif. Lockheed Martin previously delivered two SBIRS payloads that are hosted on classified satellites in highly elliptical orbits. The company is under contract to deliver a total of four SBIRS geosynchronous satellites and four hosted SBIRS payloads.

Some 43 minutes after liftoff, the United Launch Alliance (ULA)-built Atlas 5 rocket deployed the SBIRS satellite into a geosynchronous transfer orbit, the press release said. The satellite's initial orbit carries it some 200 kilometers from Earth at its closest point and 36,000 kilometers from Earth at its farthest, Jim Spornick, ULA's vice president of mission operations, said during an April 26 media briefing. The spacecraft will fire its liquid apogee engine six times over nine days to circularize its orbit at 36,000 kilometers, Jeff Smith, Lockheed Martin's SBIRS vice president and general manager, said during the briefing.

Once the satellite reaches geosynchronous orbit, it will begin a six-month check out and calibration phase before it is expected to begin delivering usable data to the

Air Force's First Dedicated SBIRS Satellite Carried to Orbit

tactical intelligence community, Air Force Brig. Gen. (select) Roger Teague, director of the Infrared Space Systems Directorate at Air Force Space and Missile Systems Center, Los Angeles, said during the briefing. U.S. Strategic Command is expected to certify the satellite for integrated theater operations in October 2012, Teague said.

Top Chinese Supercomputers Point to Aggressive HPC Strategy

April 26, 2011

Top Chinese Supercomputers Point to Aggressive HPC Strategy

Michael Feldman, HPCwire Editor

China's meteoric rise to the top of the of the supercomputing heap has generated plenty of angst in the West. At a time when government budgets in the US, Europe and Japan are being slashed, China is investing heavily in its high performance computing capability. At the most recent IDC HPC User Forum, a presentation on China's top 100 supercomputers points to how far and how fast the nation has come in a few short years.

When [China's HPC TOP100](#) was first published in 2002, the country had a total of 5 machines on the international TOP500 list. Since then, number of Chinese systems has grown steadily, with its fastest increase -- from 24 to 42 systems occurring last year. The latest rankings from November 2010 have China with the number one and number three machines -- the 2.5 petaflop Tianhe-1A and 1.3 petaflop Nebulae systems, respectively -- along with three other supercomputers in the top 100.

At the IDC HPC User Forum, Liang Yuan, of China's Laboratory of Parallel Software and Computational Science -- part of the Institute of Software, Chinese Academy of Sciences (ISCAS) -- talked about some interesting trends in the country's top supers. Perhaps most notable is China's aggressive adoption of GPU technology, which propelled the multi-petaflop Tianhe-1A to the number one spot in 2010. In fact, the country's top three systems are all heterogeneous CPU-GPU machines, based on Intel Xeon and NVIDIA Tesla processors.

Some other interesting facts from Liang Yuan's [presentation](#) (PPT):

- The aggregate Linpack performance of China's TOP100 is more than 9.6

Top Chinese Supercomputers Point to Aggressive HPC Strategy

petaflops.

- 59 percent of the systems use GigE as the interconnect; 37 percent use InfiniBand.
- Intel processors are in 80 percent of the systems; AMD processors in 19 percent.
- Quad-core CPUs dominate the list with an 81 percent share.
- The top seven systems were designed and built by Chinese manufacturers or organizations.

排名	厂商 Manufacturer	型号 Computer	安装地点 Installation Site	安装年份 Year	处理器核 Num of Proc	Linpack (Gflops)	Peak (Gflops)	效率 Efficiency
1	国防科大 NUDT	天河一号/Tianhe-1A/7168x2 Intel Hexa Core Xeon X5670 2.93GHz + 7168 Nvidia Tesla M209@1.15GHz+2048 Hex. Core FT-1000@1 GHz/私有高速网络80Gbps	国家超级计算天津中心	2010	202,752	2,507,000.00	4,701,000.00	0.533
2	曙光 Dawning	曙光星云/Dawning TC3600 Blade/Intel Hexa Core X5650+	曙光天津产业基地	2010	120,640	1,271,000.00	1,904,300.00	0.426
3	中科院过程所 IPE, CAS	Male8.5 Cluster/320x2 Intel QC Xeon E5520 2.26 GHz + 320x6 Nvidia Tesla C2050/QDR Infiniband	中国科学院过程工程研究所	2010	33,120	207,300.00	1,138,440.00	0.182
4	曙光 Dawning	魔方曙光5000A/1920x4 AMD QC Barcelona 1.9GHz/DDR Infiniband/WCCS+Linux	上海超级计算中心	2008	30,720	180,600.00	233,472.00	0.774
5	联想 Lenovo	深超200Y1240x2 Intel Xeon QC E5450 3.0GHz/140x4 Intel Xeon QC X7350 2.93GHz Infiniband 4xDDR	中国科学院超级计算中心	2008	12,160	106,500.00	145,293.00	0.733
6	曙光 Dawning	曙光星云/Dawning TC3600 Blade/220x2 Intel Hexa Core X5650 + 1 Nvidia Tesla C2050/QDR Infiniband	成都超级计算中心(二期)	2010	5,720	76,350.38	141,389.60	0.540
7	曙光 Dawning	生物+带机/Dawning TC3600 Blade/Intel Hexa Core X5650+ Nvidia Tesla C2050 GPU/QDR Infiniband	中国科学院计算技术研究所	2010	4,160	55,527.55	102,628.80	0.540
8	IBM	xSeries x3650M2 Cluster/Intel Xeon QC E55xx 2.53 GHz/Giga-E	工程公司	2010	8,960	51,200.00	90,680.00	0.565
9	HP	Clustr Platform 300 BL460c G6/Intel Xeon E5540 2.53 GHz/Giga-E	中国电信	2010	7,848	41,880.00	79,420.00	0.527
10	IBM	BladeCenter HS22 Cluster/Intel Xeon QC Q1 2.53 GHz/Giga-E	网络公司	2009	7,168	41,270.00	72,540.00	0.569

The application set for these systems is pretty much on par with other high-end supercomputers around the world. Energy, industrial and research codes are the top three applications, running on 17 percent, 15 percent, and 12 percent of these TOP100 systems, respectively. Gaming applications, surprisingly, are hosted on 9 percent of the machines, representing the same proportion as government apps. Other HPC applications, including telecom, weather, biotech, finance, and a handful of others, are present in less amounts. It's not clear how accurate this application breakdown really is since it doesn't appear to account

Top Chinese Supercomputers Point to Aggressive HPC Strategy

for multiple application types running on the same system.

Where the China TOP100 machines diverge most noticeably from other countries (besides the US, that is) is the proportion of systems built domestically. Overall, about half the systems, 51 percent to be exact, are derived from US-based vendors, with the remaining 49 percent built by Chinese manufactures. IBM and HP dominate the foreign OEMs, with a 28 percent and 19 percent share, respectively. Dell at 3 percent and Sun Microsystems (Oracle) at 1 percent are the only other two that show up on the list.

Looking at the domestic manufacturers, Dawning owns the lion's share of the TOP100 market, with 34 percent of all systems. Lesser-known server makers Inspur (5 percent), Lenovo (3 percent), Sunway (3 percent), and PowerLeader (2 percent) contribute much less to this elite tier.

Two of China's largest machines were constructed by government organizations, in this case, the National University of Defense Technology (NUDT), which designed and built the top-ranked 2.5 petaflop Tianhe-1A supercomputer (which features a home-grown system interconnect), and the Chinese Academy of Sciences' Institute of Process Engineering, which developed the 207-teraflop Mole 8.5 cluster. Whether this becomes a systems development model for future machines, or it goes the more traditional route of vendor collaborations remains to be seen. But right now the Chinese government stands alone as an HPC OEM.

It's worth noting that these two government machines represent a big chunk of the FLOPS on the nation's TOP100 -- greater than the aggregate capacity contributed by Dawning and the other Chinese manufacturers, and more than twice the capacity of the US-built machines. Overall, the top supers build domestically deliver 5.052 petaflops, with the imports contributing a relatively modest 1.18 petaflops.

Top Chinese Supercomputers Point to Aggressive HPC Strategy

That skewed distribution illustrates China's broader strategy for developing its supercomputing infrastructure, that is, develop indigenous system expertise and capability and lessen its reliance on imports. That approach will eventually work its way down to the CPU level. To date, Chinese supercomputing has relied almost exclusively on chips from Intel, AMD and NVIDIA.

The big push right now is to get the domestically-designed Godson CPU technology deployed in supercomputers. Godson (aka Loongson) is a MIPS-based processor family, developed by the government-backed Institute of Computing Technology (ICT) in the Chinese Academy of Sciences. Starting in 2002, the Godson designs have slowly worked their way up the performance ladder, adding 64-bit capability in 2006. In 2007, a supercomputer with the name of KD-50-I was constructed, using 336 Godson-2F processors to deliver one teraflop of performance.

At a presentation at International Solid State Circuits Conference (ISSCC) in February, Godson lead engineer Weiwu Hu [revealed](#) that the Godson-3B will be the CPU in the upcoming 300-teraflop Dawning machine slated for installation this summer. These are 8-core chips, designed to deliver at 128 raw gigaflops at just 40 watts, and are said to rival the best US-made processors in power-efficiency and performance.

While it may take a few chip generations for the Godson processors to become a force in Chinese HPC, the country's direction has become clear: to become a major player in supercomputing from top to bottom, and do so with native capability. Liang Yuan's IDC presentation ended with a couple of predictions, namely that China intends to deploy a 10-petaflop Linpack system in the 2012 to 2103 timeframe and a 100-petaflop machine two years later.

That would almost certainly keep pace with the top systems in the US and outrun European-based machines by at least a year or two. More importantly, China appears to be determined to have a US-like presence in supercomputing,

Top Chinese Supercomputers Point to Aggressive HPC Strategy

building not just a top-tier infrastructure, but an HPC industry as well. This has generated plenty of nervousness in the US HPC community, who sees its leadership threatened. A recent [address by Dona Crawford](#), associate director for Computation at LLNL, sums the feeling rather well:

So it's not that I want to beat China per se; it's that I want us to have parity with them. I don't want to rely on them for the chip technology embedded in the supercomputers we use for national security. I don't want to rely on them for the low level software that runs my supercomputer because they figured out the parallelism before we did. I don't want to rely on them, or anyone else, for my own standard of living, for my safety and security, for the inventions that propel us forward, for open dialog and communications, all of which rely on supercomputing. I want the U.S. to be self reliant, capable and responsible for our own prosperity.

Intel Increases Transistor Speed by Building Upward

Intel Increases Transistor Speed by Building Upward

By JOHN MARKOFF

Published: May 4, 2011

HILLSBOROUGH, Ore. — Intel announced Wednesday that by building a key portion of a microprocessor's transistor above the chip's surface, it has found a way to make smaller, faster and lower-power computer chips.

Intel intends to break with the basic design of the so-called planar transistor that has remained a constant in the chip industry since 1959 when Robert Noyce, Intel's co-founder, and Jack Kilby of [Texas Instruments](#) independently invented the first integrated circuits.

Since the advent of the microchip, the transistor, which is the electronic switch that is the basic building block of the information age, has been manufactured in just two dimensions.

But now, when the space between the billions of the tiny electronic switches on the flat surface of a computer chip is measured in the width of just dozens of atoms, designers are increasingly turning to the third dimension to find more room.

The company has already begun making its microprocessors using this new 3-D transistor design called a FINFET (for fin field-effect transistor), which is based around a remarkably small pillar, or fin, of silicon that rises above the surface of the chip. Intel, based in Santa Clara, Calif., plans to enter general production based on the new technology some time later this year.

Although the company will not give technical details about its new process in its Wednesday announcement, it said that it expected to be able to make chips that run as

Intel Increases Transistor Speed by Building Upward

much as 37 percent faster in low-voltage applications and it would be able to cut power consumption as much as 50 percent.

Intel currently uses a photolithographic process to make a chip, in which the smallest feature on the chip is just 32 nanometers, a level of microscopic manufacture that was reached in 2009. (By comparison a human red blood cell is 7,500 nanometers in width and a strand of DNA is 2.5 nanometers.) “Intel is on track for 22-nanometer manufacturing later this year,” said Mark T. Bohr, [an Intel senior fellow](#) and the scientist who has overseen the effort to develop the next generation of smaller transistors.

The company’s engineers said that they now feel confident that they will be able to solve the challenges of making chips through at least the 10-nanometer generation, which is likely to happen in 2015.

The timing of the announcement Wednesday is significant, Dr. Bohr said, because it is evidence that the world’s largest chip maker is not slipping from the pace of doubling the number of transistors that can be etched onto a sliver of silicon every two years, known as Moore’s Law. Although not a law of physics, the 1965 observation by Intel co-founder Gordon Moore has defined the speed of innovation for much of the world’s economy. It has also set the computing industry apart from other types of manufacturing because it has continued to improve at an accelerating rate, offering greater computing power and lower cost at regular intervals.

However, despite its promise and the company’s bold claims, Intel’s 3-D transistor is still a controversial technology within the chip industry. Indeed, a number of the company’s competitors believe that Intel is taking a multibillion-dollar gamble on an unproven technology that could be a disastrous decision.

There has been industry speculation that FINFET technology will give Intel a clear speed

Intel Increases Transistor Speed by Building Upward

advantage, but possibly less control over power consumption than alternative approaches.

By opting for a technology that emphasizes speed over low power, there is still the possibility that Intel could win the technology battle and yet lose the more important battle in the marketplace. The scope of Intel's gamble is underscored by the fact that while the company dominates in the markets for data center computers, desktops and laptops, it has largely been locked out of the tablet and smartphone markets which are growing far more quickly than the traditional PC industry. Those devices use ultra-low-powered chips in order to conserve battery power and reduce overheating. [Apple](#), for example, uses Intel's microprocessors for its desktops and laptops, but for the [iPhone](#) and [iPad](#) it has chosen to use a rival low-power design built by others that Apple originally helped pioneer in the late 1980s.

Industry executives and analysts have said that Intel is likely to have a full generation lead over its rivals in the shift to 3-D transistors. For example, T.S.M.C., the Taiwan-based chip maker, has said that it does not plan to deploy FINFET transistor technology for another two years.

Other companies, like ST Microelectronics, are wagering that an alternative technology based on placing a remarkably thin insulating layer below traditional transistors will chart a safer course toward the next generation of chip manufacturing. They believe that the insulation approach will excel in low-power applications and that could be a crucial advantage in consumer-oriented markets where the vast majority of popular products are both handheld and battery-powered.

“Silicon-on-insulator could be a win in terms of power efficiency,” said David Lammers, the editor in chief of [Semiconductor Manufacturing & Design Community](#), a Web site.

“From what I am hearing from the S.O.I. camp, there is a consensus and concession that

Intel Increases Transistor Speed by Building Upward

FINFETs are faster. That's the way you want to go for leading edge performance." In a factory tour here last week, Intel used a scanning electronic microscope to display a computer chip made using the new 22-nanometer manufacturing process . Viewed at a magnification of more than 100,000 times, the silicon fins are clearly visible as a series of walls projected above a flat surface. It is possible to make transistors out of one or a number of the tiny fins to build switches that have different characteristics ranging from faster switching speeds to extremely low power. Stepping back and looking at the chip under lower power magnification, it is possible to see the wiring design that appears much like a street map displaying millions of intersections.

Despite the impressive display, Intel's executives acknowledge the challenge the company is facing in trying to catch up in the new consumer markets that so far have eluded it.

"The ecosystem right now is not aligned in our favor," said Andy D. Bryant, Intel's chief administrative officer who now runs the company's technology and manufacturing group. "It has to be good enough for the ecosystem to take notice and say, 'we better pay attention to those guys.' "

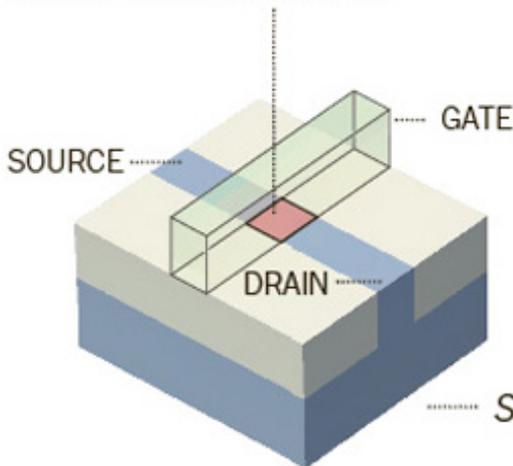
Intel Increases Transistor Speed by Building Upward

New Transistor Grows in the Third Dimension

The new Intel transistor provides higher performance by increasing the conductive area between the source and drain regions of the chip, allowing more current to flow through.

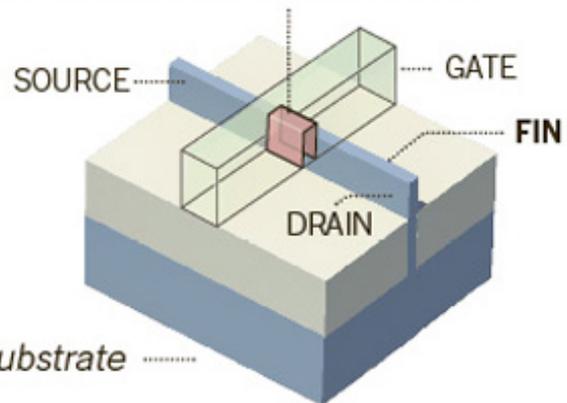
TRADITIONAL TRANSISTOR

Planar **conductive area**



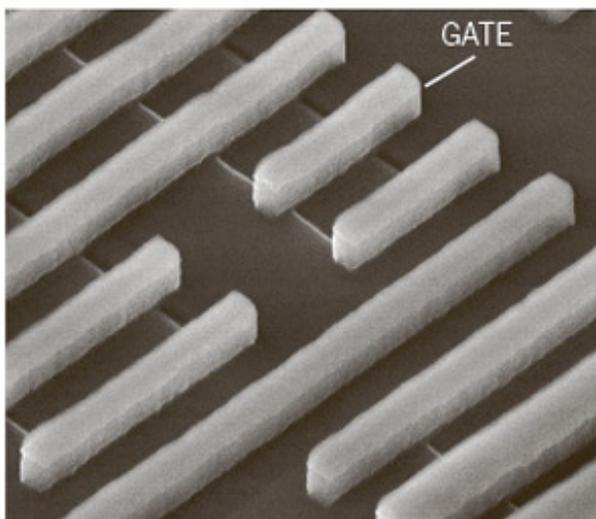
NEW INTEL TRANSISTOR

Conductive area is expanded on **three sides of a raised fin**



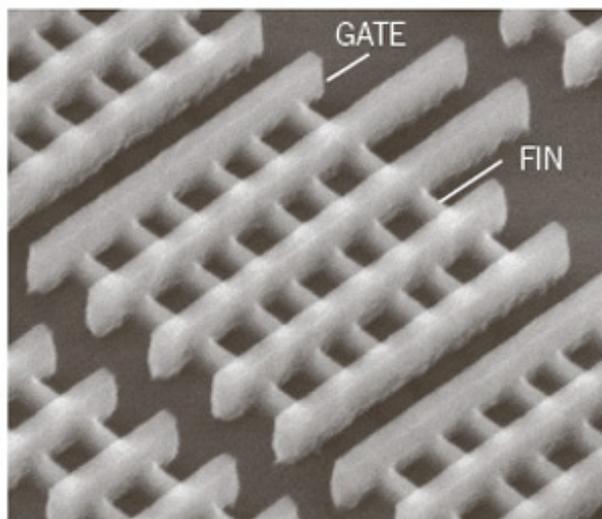
The new transistor with its raised **fin** requires a smaller footprint, allowing more of them to fit in a computer chip. The new design can also reduce power consumption, yielding better battery life on devices.

Traditional planar transistor



Source: Intel

Intel Tri-Gate transistor



THE NEW YORK TIMES

Intel Increases Transistor Speed by Building Upward

How Three-Dimensional Transistors Went from Lab to Fab

Friday, May 6, 2011

How Three-Dimensional Transistors Went from Lab to Fab

The story behind Intel's new design.

By Katherine Bourzac

Intel's new [three-dimensional transistor design](#), announced early this week, is the culmination of more than a decade of research and development work that began in a lab at the University of California, Berkeley in 1999.

The 22-nanometer transistors, which Intel says will make chips 37 percent faster and half as power hungry, will be used for every element on the company's 22-nanometer scale chips, including both the logic and memory circuits. Processors that use the "tri-gate" transistors have been demonstrated in working systems, and the company will begin volume production in the second half of this year. It's unclear just how device-makers will take advantage of the chips, but they're likely to enable improved battery life and greater sophistication for portable devices, as well as faster processing for desktops and servers.

Intel turned to the new design because existing designs have begun running up against a performance roadblock. Conventional transistors are made up of a metal structure called a gate that's mounted on top of a flat channel of silicon. The gate controls the flow of current through the channel from a source electrode to a drain electrode. With every generation of chips, the channel has gotten smaller and smaller, enabling companies like Intel to make faster chips by packing in more transistors. But it has become more difficult for the gate to fully cut off the flow of current. Leaky transistors that don't turn off completely waste power.

The tri-gate transistors use rectangular silicon channels that stick up from the surface of the chip, allowing the gate to contact the channel on three sides, instead of just one. This more intimate contact means the gate can turn the transistor off nearly completely even at the 22-nanometer scale, which is responsible for the energy-efficiency gains in Intel's new chips. It's also possible to make tri-gate transistors with more than one silicon channel connected to each gate in order to increase the amount of current that can flow through each transistor, enabling higher performance.

Intel didn't invent this transistor design, but the company is the first to get it into production. If the company had stuck with planar transistors in the move from 32- to 22-nanometer transistors, the chips would have demonstrated 20 to 30 percent gains in

How Three-Dimensional Transistors Went from Lab to Fab

efficiency and performance, says industry analyst [Linley Gwennap](#). There had been speculation that the company would use the new transistor design for memory elements and not logic, and so not completely eliminate the planar transistors. By using the tri-gate technology for both memory and logic, says Gwennap, "Intel is really surging for the fences and seeing a large improvement in performance, which could be a huge advantage" over its competitors.

These three-dimensional transistors were first imagined and built by three researchers at the University of California, Berkeley, in the late 1990s, in response to a call from the United States Defense Advanced Research Projects Agency for designs that would allow transistors to scale below 25 nanometers, an order of magnitude smaller than the ones in production at the time. [Chenming Hu](#) wrote out the technical specs for the new transistor on a plane ride to Japan in 1996. A Berkeley group made up of Hu, [Jeffrey Bokor](#), and [Tsu-Jae King Liu](#) first made these transistors, which they called FinFETs, in 1999.

"It was an instant hit," says Hu. The university opted to release the intellectual property into the public domain instead of patenting it; as the Berkeley researchers kept refining the designs, Hu presented the work at several companies, including Intel. By 2002, the FinFET and a second Berkeley design, known as "silicon on insulator," were the devices favored by the [International Technology Roadmap of Semiconductors](#) as the technologies likely to meet the industry's needs in the next 15 years. But at Intel, at least, FinFET pulled ahead of the second design, which relies on adding a very thin layer of silicon to a transistor. Until about two years ago, the companies who make silicon wafers weren't able to make the active layer thin enough. French company [Soitec](#) can now manufacture the necessary wafers for this alternate design, and Hu says Intel's competitors may at some point adopt it.

Getting the promising three-dimensional device design out of the lab and into production took about a decade. Intel hasn't disclosed many of the details of what fab upgrades are necessary to make the new transistors, but based on the fact that no new materials or machines are apparently required—and the marginal increase in production cost of 2 to 3 percent promised by the company—the changes appear to be minor. The company has said that making the three-dimensional channels only involves an extra etching step.

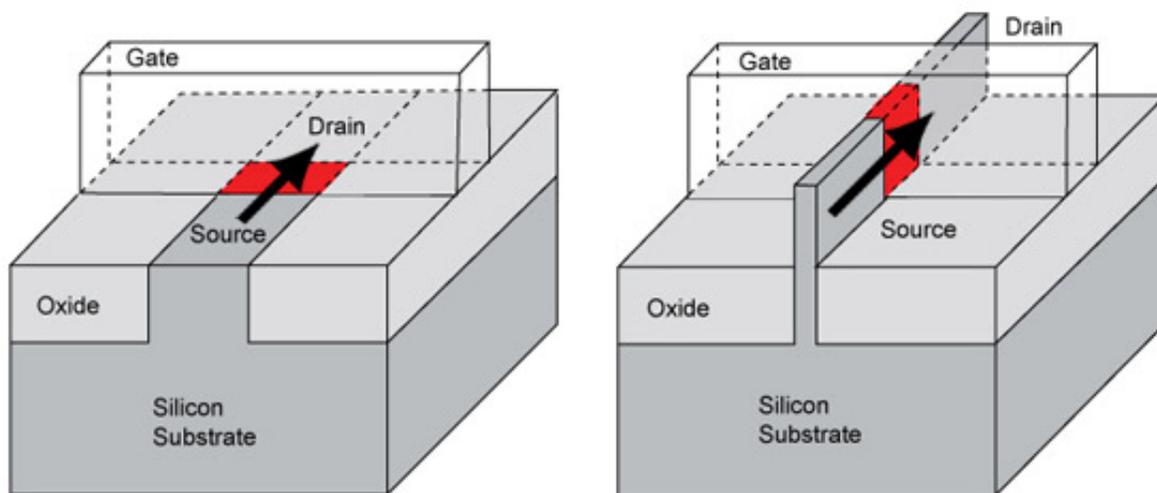
Hu says the Berkeley researchers decided from the start that their new design would have to be compatible with the industry's existing infrastructure, and that has proved to be the case. The main hurdle in getting the technology ready for volume production, says Hu, was likely dealing with reliability: getting the dimensions of the very thin

How Three-Dimensional Transistors Went from Lab to Fab

channel under control when billions of them must be made on every single wafer.

Hu says the Berkeley group designed these transistors so that they would not require circuit designers to completely redesign chip architectures. That's part of the reason why Intel can get products out so quickly. Hu's group has been working on circuit-simulation tools for the tri-gate transistors for the past five years.

Still, circuit designers see new opportunities that could open up with these transistors. They offer new ways of tuning the behavior of individual gates, which "gives designers new knobs to play with in order to further improve power efficiency and reliability," says **Subhasish Mitra**, professor of electrical engineering and computer science at Stanford University. Seeing a totally new transistor go into volume production within the span of about a decade is an encouraging sign that the industry "is not stale" and that good technology ideas can still make it out of academic labs, Mitra adds.



Moving up: In a conventional transistor (left) a top-mounted gate controls the flow of electrical current through a flat silicon channel below. In Intel's new design (right) the silicon channel is raised like a fin, so that the gate contacts it from three sides. This provides greater control over the flow of current through the channel, and reduces power leakage.

Credit: *Technology Review*

How Three-Dimensional Transistors Went from Lab to Fab

Copyright Technology Review 2011.

