# Index

## Cyber Bytes - 8 JUL 11

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

**Links of interest:**

**Leading IT organization org charts:** <http://www.cultofmac.com/apple-ms-google-etc-imagined-as-fun-org-charts/102917?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+cultofmac%2FbFow+%28Cult+of+Mac%29>

**NIST Supply Chain Risk Management Knowledge Library**: <http://scrm.nist.gov/Knowledge%20Base.html>

**Cloud Computing**

**Microsoft Challenges Itself in the Clouds**
-<http://online.wsj.com/article/SB10001424052702304231204576405563616351454.html?mod=WSJ_Tech_RIGHTTopCarousel_1>

**There's a Big Thing Missing From Microsoft Office 365**
-<http://blogs.forbes.com/quickerbettertech/2011/06/27/theres-a-big-thing-missing-from-microsofts-office-365/?partner=yahootix>

**Microsoft Plugs Cloud to Feds**
-<http://www.nextgov.com/nextgov/ng_20110701_8120.php>

**Cyber Security**

**Dissolution of Hacker Group May Not End Attacks**
-<http://www.nytimes.com/2011/06/27/technology/27hack.html?partner=rss&emc=rss&pagewanted=print>

**A Stronger Net Security System Is Deployed** [DNSSEC]
-<http://www.nytimes.com/2011/06/25/science/25trust.html>

**TDL-4: The 'Indestructible' Botnet**
-<http://news.cnet.com/8301-13506_3-20075725-17/tdl-4-the-indestructible-botnet/?part=rss&tag=feed&subj=News-Security>

# Index

**Security Researchers Discover 'Indestructible" Botnet**
-<http://www.bbc.co.uk/news/technology-13973805>

**A Smarter, Stealthier Botnet**
-<http://www.technologyreview.com/computing/37945/?ref=rss&a=f>

**A 'Futures' Market for Computer Security**
-<http://www.technologyreview.com/computing/37967/?ref=rss&a=f>

**Former CIA Director: Build a New Internet to Improve Cybersecurity**
-<http://www.nextgov.com/nextgov/ng_20110706_1137.php>

**Threat of Destructive Coding in Foreign-Manufactured Technology Is Real**
-<http://www.nextgov.com/nextgov/ng_20110707_5612.php>

**Symantec Compares iOS and Android Security**
-<http://www.macworld.com/article/160801/2011/06/smartphone_security.html#lsrc.rss_main>

**Cyber War**

**US Military Expanding Arsenal of Cyber-Warfare Capabilities**
-<http://www.eweek.com/c/a/Security/US-Military-Expanding-Arsenal-of-CyberWarfare-Capabilities-389786/>

**Lessons From Estonia: Preparing for a Major Cyberattack** [videos]
-<http://www.nextgov.com/nextgov/ng_20110706_9154.php>

**DoD**

**Navy Cyber Unit Scans Horizon For New Challenges**
-<http://defensesystems.com/articles/2011/06/08/cyber-defense-navy-cyber-programs.aspx>

**Navy Vows to Fight for Its Superlaser, Hypersonic Gun**
-<http://www.wired.com/dangerroom/2011/06/navy-vows-to-fight-for-its-superlaser-hypersonic-gun/>

**US Soldiers Push Network in Desert Trials**
-<http://www.defensenews.com/story.php?i=6944673&c=LAN&s=TOP>

# Index

**Giant Spy Blimp Could Decide Surveillance's Future**
-<http://www.wired.com/dangerroom/2011/07/spy-blimp-battle/>

**Army's Antennae in the Sky**
-<http://www.dodbuzz.com/2011/07/07/the-armys-antennae-in-the-sky/>

Related to the above two stories: **Airships for the 21st Century**
-<http://spectrum.ieee.org/aerospace/aviation/airships-for-the-21st-century/0>

**UCAS Demonstrator Clears Key Milestone in Sea-Based Qualification Testing**
-<http://www.defensedaily.com/publications/dd/14443.html>

**Aegis ACB-12 Passes Live Aircraft-Tests**
-<http://rpdefense.over-blog.com/article-aegis-acb-12-passes-live-aircraft-tests-78687958.html>

**DoD CIO Duties *Not* Going to Cyber Command**
-<http://www.fiercegovernmentit.com/story/dod-cio-duties-not-going-cyber-command/2011-07-05?utm_medium=rss&utm_source=rss>

**Army Network Exercise Will Shake Up Status Quo, Says Vice Chief Gen. Chiarelli**
-<http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?List=7c996cd7%2Dcbb4%2D4018%2Dbaf8%2D8825eada7aa2&ID=457>

**DoD Wants to Shift $920M for Intel Efforts**
-<http://www.defensenews.com/story.php?c=POL&i=7034730&s=TOP>

## Information & Society

**Global Tech Leaders Promote Open Internet**
-<http://www.informationweek.com/news/government/leadership/231000991>

**US and Russia Among 22 Nations Supporting International Cyber Resolution**
-<http://www.nextgov.com/nextgov/ng_20110705_7349.php>

**Judge Rules Against Google in Street View 'Wi-Spy' Lawsuit**
-<http://www.macworld.com/article/160926/2011/07/google_streetview.html>

## Information Technology

**Agencies Face Challenges Developing Systems for Multiple Mobile Operating**

# Index

**Systems**
-<http://www.fiercegovernmentit.com/story/agencies-face-challenges-developing-multiple-mobile-operating-systems/2011-06-27?utm_medium=rss&utm_source=rss>

**Are We Ready For the Era of .Anything?**
-<http://www.technologyreview.com/web/37895/?ref=rss>

**World's Data Will Grow by 50X in Next Decade, IDC Study Predicts**
-<http://www.computerworld.com/s/article/9217988/World_s_data_will_grow_by_50X_in_next_decade_IDC_study_predicts>

**'Geeky' World of IT Loses Its Appeal as a Career Choice**
-<http://womenatthetop.ft.com/articles/women-top/12623ca4-a636-11e0-8eef-00144feabdc0>

**Storage Wars:  Web Growth Sparks Data-Center Boom**
-<http://online.wsj.com/article/SB10001424052702303763404576417531646400002.html?mod=WSJ_Tech_LEFTTopNews>

**Spy Geeks Want Holodeck Tech for Intel Analysts**
-<http://www.wired.com/dangerroom/2011/07/spy-geeks-holodeck/>

**Why Lithium Ion Batteries Die So Young**
-<http://gigaom.com/cleantech/why-lithium-ion-batteries-die-so-young/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheAppleBlog+%28GigaOM%3A+Apple%29>

## Robotics

**Navy Orders Study on UCLASS Concepts**
-<http://www.dodbuzz.com/2011/06/27/navy-orders-study-on-uclass-concepts/>

**Global Race On to Match US Drone Capabilities**
-<http://www.washingtonpost.com/world/national-security/global-race-on-to-match-us-drone-capabilities/2011/06/30/gHQACWdmxH_story.html>

**Have US Drone Wars Opened a Pandora's Box?**
-<http://www.dodbuzz.com/2011/07/05/have-u-s-drone-wars-opened-a-pandoras-box/>

**'Hands-free' Landing Is a Step Toward Unmanned Naval Flight**

-<http://hamptonroads.com/2011/07/handsfree-landing-step-toward-unmanned-naval-flight>

**A Roboticist's Trip From Mines to the Moon**
-<http://online.wsj.com/article/SB10001424052702304569504576405671616928518.html>

**Space**

**NASA IG Warms of Possible Weather Satellite Coverage Gap**
-<http://www.fiercegovernmentit.com/story/nasa-ig-warns-possible-weather-satellite-coverage-gap/2011-07-06?utm_medium=rss&utm_source=rss>

**Technology Advances**

**This 45-Mile "Wi-Fi" Could Connect a Smarter Power Grid**
-<http://www.technologyreview.com/computing/37881/?ref=rss&a=f>

**Real US Stealth-Tech Advantage: Its Assembly Lines**
-<http://www.wired.com/dangerroom/2011/07/stealth-advantage/>

**Moore's Law Meets Exascale Computing**
-<http://www.hpcwire.com/hpcwire/2011-06-29/moore_s_law_meets_exascale_computing.html>

**IBM Announces Computer Memory Breakthrough**
-<http://www.computerworld.com/s/article/9218031/IBM_announces_computer_memory_breakthrough>

**Making Speedy Memory Chips Reliable**
-<http://www.technologyreview.com/computing/37915/?ref=rss>

**Graphene Enables Invisibility Cloak**
-<http://spectrum.ieee.org/nanoclast/semiconductors/nanotechnology/graphene-enables-invisibility-cloak>

**The Secret Life of White-Space Radio**
-<http://news.cnet.com/8301-1035_3-20076127-94/the-secret-life-of-white-space-radio/>

## Microsoft Challenges Itself in the Clouds

By STEVEN D. JONES

Microsoft Corp. will introduce a cloud version of its Office applications this week, a move that ramps up the software giant's competition not only with companies such as Google Inc. and VMware Inc. but with itself.

On Tuesday, Microsoft Chief Executive Steve Ballmer is scheduled to launch Office 365, a combination of communication, collaboration and productivity software delivered via the Internet. Microsoft, which is holding an event in New York to celebrate the debut, calls the suite of services the "next generation cloud service."

Office 365 enters a crowded field. Google Docs from Google and VMware's Zimbra email, for example, are attracting hundreds of companies seeking tools that work from desktop computers, smartphones or the growing number of tablet computers in use today.

Microsoft's biggest competitor, however, might be itself. Nearly nine of every 10 office computers runs one of the 14 versions of Office the company has released since the software's launch in 1989. The company now needs to convince those computer users, estimated at about one billion, to switch to Office in the cloud without disrupting the legacy version that is financing the transition.

It's a changeover Microsoft has to make. More people want to be able to use mobile devices for work. That allows them to make any environment their office, but requires corporate IT departments to coordinate a growing array of hardware.

Cloud services are growing, in part, because they address this dynamic, providing the most cost-effective way to link all those gadgets.

Microsoft also sees profit in the cloud. The market for cloud-computing

services and software is expected to grow more than 27% annually over the next five years and reach $73 billion by 2015, International Data Corp. projected last week.

Cloud computing, which uses networks of computers to store and deliver applications and content, will power a wave of technology expansion, says IDC's vice president and chief analyst, Frank Gens.

Like the mainframe and personal computers before it, cloud software and services "are merging into the industry's third major platform for long-term growth," said Mr. Gens. He estimates that by 2015 one of every seven dollars spent on technology will be connected with cloud computing and "the winners of the cloud platform wars will likely be the new power brokers of the IT industry."

Microsoft was the power broker in the PC era, but whether it's able to get on top of the cloud will likely depend on what Mr. Ballmer introduces Tuesday.

Office 365 blends many existing Microsoft utilities, which currently are offered online à la carte, into a single cloud offering. In a major break with the packaged-software era, customers will be able to buy only what they need. A small company, for example, can subscribe to Office 365 for as little as $2 a month for each worker accessing email and little else. An enterprise user who needs the full suite of Office software will pay about $27 a month.

By comparison, the packaged version of Office 2010 for Home & Business retails for $210 at Amazon.com. Office 2010 Professional retails for $408.

Such metered pricing also eases the transition for users running older versions of Office on desktop systems, allowing them to get new features for their mobile devices without the cost of full conversion.

The pricing model also allows Microsoft to generate new recurring revenue

from customers who are content with older software.

To sweeten the deal for its biggest clients, Microsoft earlier this year modified its agreements with its largest corporate customers that grant licenses to companies with thousands of users. The changes allow maximum flexibility to switch users from license use, which covers the use of software on company computers, to the cloud service. The feature could allow clients months of Office 365 usage free until their corporate agreements come up for renewal.

Like all cloud providers, Microsoft faces risks. That was evident one morning recently when some subscribers to current Microsoft online services in the Americas region experienced intermittent outages. Other companies, like Amazon, have experienced similar outages.

And while Microsoft has been adjusting its strategy, cloud pioneers such as San Francisco-based Salesforce.com Inc. and Seattle-based Amazon have forged ahead.

Salesforce.com has added a communication technology called Chatter to its service to allow clients to communicate within its sales management cloud service. Amazon's Elastic Cloud has attracted enterprise customers because of its ability to scale up capacity to match peaks in client demand. And Microsoft's biggest rival, Google, is encroaching on Microsoft's core Office franchise with the spread-sheet and word-processing utilities within its Google Docs cloud service.

By 2015, IDC estimates that software-oriented cloud services will account for roughly three-quarters of all spending on public cloud services.

So even though Microsoft isn't first to the party, the trend in cloud computing is leading to Microsoft's strong suit—developing software.

The introduction of Office 365 may look like a defensive move to some

people, but it also could be coming at just the right time.

# There's a Big Thing Missing From Microsoft Office 365

There's A Big Thing Missing From Microsoft's Office 365

Jun. 27 2011 - 8:32 am
*posted by* **GENE MARKS**

Image by emme-dk via Flickr

This week marks a significant moment in the history of technology. Microsoft is taking its biggest leap ever into "the cloud" by launching its Office 365 service. We've seen this before. In a way it's like history repeating itself.

For example in the mid 1980's when I first graduated college and entered the corporate world WordPerfect was the big name in word processing and Lotus 1-2-3 was the spreadsheet of choice. And then Microsoft entered the market with Windows and its original Office product suite. Within a few short years both WordPerfect and Lotus 1-2-3 were almost completely knocked out of the marketplace. Soon after that Microsoft turned its attention to the web. At the time, Netscape's Navigator was the only browser in town. Until 1995 and the introduction of Internet Explorer. Same thing again. After only a few short years Microsoft's browser took most of the surfing marketplace away from its main competitor.

WordPerfect, Lotus 1-2-3 and Netscape Navigator were good applications at the time. But their customers were swallowed up by a more aggressive competitor. Microsoft crushed them with a boatload of marketing dollars and a desktop computing monopoly. Those were simpler days. Now we remember those programs wistfully, like we remember Bob Geldof, Ronald Reagan and Kirk Gibson.

Today, the world of online office applications has been ruled mostly by Google Apps with some credible offerings from smaller companies like Zoho and OpenOffice. These

applications, like WordPerfect and Navigator of days gone by are also popular and full of functionality. Google's offerings, for example, are free for individuals and cost about $50 per year per user for corporate deployments. For this amount you get a whole bag of goodies, like word processing, spreadsheets, presentations, calendar and e-mail. And they're all shared together in a hosted environment for employees to collaborate and communicate.

Will Office 365 repeat Microsoft's historical success this time in the cloud marketplace? Will we see leading products like Google's Apps for Business fall into obscurity like WordPerfect, Lotus 1-2-3 and Netscape Navigator? Will we one day look back on the year 2011 with fond memories of high real estate values in Florida, cold winters in New England and Google's one-time dominance of the cloud?

It's possible. Microsoft's done it before. And Office 365 has certainly got the firepower to help them do it again.

The online versions of Word, Excel, PowerPoint and Access seem every bit as good as their desktop counterparts. The gigabytes of space offered allow us to save almost limitless amounts of databases and documents. The ease of switching between our local and online systems should keep the training curve low, even amongst the least tech-savvy. And the price of Office 365, at $6 per month per user which includes the Office web app, Exchange and SharePoint, is designed to keep small businesses like mine from even considering a switch to those evil search engine guys.

And Microsoft's got the market (and marketing) muscle too. There are more than a billion users of its Office products worldwide. A billion. And there are billions more in Microsoft's bank accounts ready to be spent on research, development, sales and

marketing to make their core cloud based offerings part of the business community's vernacular, whether we like it or not. For better or worse, we've known Microsoft for more than twenty years. We've relied on the company's software products to help us calculate the least amount we can pay our salespeople, made our presentations appear like we know what we're doing and helped us create lucrative executive employment agreements without the prying eyes of our employees knowing about them. Because of this we're pretty loyal.

But there's a problem. Office 365, the company's flagship cloud-based offering, is missing something. Something big.

Is there a hidden Easter egg in Access that explains the ending to "Inception"? Will people actually need to know the difference between "there" and "their" when typing out a simple letter? Will executives no longer have the ability to insert funny videos in their PowerPoint presentations to mask the fact that they suck as a speaker? No, no. Office 365 appears to have most, if not all, of these popular features that we're used to having in our current desktop versions.

What's missing in Office 365, Google's Business Apps and all the other cloud based "services" that software companies like Microsoft are scrambling to get on the market is something much more critical to a business like mine. It's missing my applications.

Believe it or not, my business (like most businesses) runs on other systems that are not Microsoft's. Sure, we use Office 2010. But our accounting system is QuickBooks and our customer relationship management system is GoldMine. We use Adobe's PDF software and Mozilla Firefox. Our clients use other CRM packages and run their businesses on vertical applications suited to their industry. Many of them have internal applications

that they've created to manage their specialized inventories or monitor their manufacturing processes.

These applications are all stored in different places too. Some are on servers inside of our offices and factories. Others are located halfway across the world, at company owned facilities in Europe or Asia and accessed through our virtual private networks. Some are now hosted by cloud based providers. Other applications are rented via a software-as-a-service model.

Office 365 isn't solving this problem. It's still a mess. Data is all over the place. It's now just another place for employees to access Word and store files. It's just a...place. Like our servers are just a place. Except this place is on Microsoft's servers. For some that may be a benefit. For others it won't make much of a difference.

That's because most companies' applications, custom programs and databases were all created by different people. Hot shot programmers drinking Red Bulls. Established software vendors. Nerdy internal engineers anticipating the upcoming release of "Mass Effect 3" (where "Earth itself is attacked by ancient machinery and humanity yet again faces the biggest threat in the galaxy."). Some of these programs work better than others. Some need a lot of support and tender loving care to keep working effectively. These applications were written for specific purposes over many years. They work well on the servers they're on, but may stop working altogether if moved to another box.

And none of them really integrate. Oh sure, some companies with lots of dollars to spend and plenty of alcohol on hand have created scripts to pull data from one disparate

system and jam it into another disparate system from some type of ASCII file that's generated overnight. And this works for them...about 90% of the time. But most of us are still keying in the same data two, three, even four times into different systems. We've got invoices created in Microsoft Word that have the same data from our accounting system except our accounting system can't generate the data in the format we like to see it in. And we've got spreadsheets with the same information that's in our inventory control database.

Microsoft's big jump into the cloud isn't really helping my office. It's helping Microsoft compete against Google and add a new future revenue stream which can then be multiplied many times over by a team of Wall Street analysts as they re-calculate the company's long term value. I can access Word or Excel online now using remote desktop or products like GoToMyPC or LogMeIn .

What's missing from Office 365 is the office. And my applications in my office. In the old days, a software company could get away with denying hardware issues by saying "hey man...we're just a software company. We can't be responsible for your network." That mindset needs to change.

Because in today's cloud based world the winning software company will take ownership of all software applications, and the environment that they're in too. Microsoft would *kill* Google if it stopped calling itself a software company and started behaving like a true office productivity company. Take your software, and my software, and host it ALL on your servers. Take ownership for how it works together. Integrate it better. Make it work faster. It's the cloud guys. You don't have to blame the infrastructure anymore. You can now own it, control it, collaborate with other vendors and make your

applications (and other people's applications) work better within it.

That way Microsoft would truly be using the cloud to solve problems...and separate itself from everyone else.  Office 365 is missing that.

# Microsoft Plugs Cloud to Feds

## Microsoft plugs cloud to feds

BY JOSEPH MARKS 07/01/2011

Microsoft officials are touting the company's new cloud-based Office 365 as a good choice for federal customers because of its tiered subscription structure and secure management.

Office 365, unveiled at an event Tuesday in New York, is an updated version of the software giant's Business Productivity Online Standard Suite and includes improved, Web-based versions of its word processing, collaboration, PowerPoint, email, calendar and instant messaging products.

BPOS received the coveted Federal Information Security Management Act certification from the Agriculture Department in April, after which the agency agreed to migrate about 120,000 employees to the cloud-based suite.

The Office 365 package Microsoft is offering to federal users includes isolated cloud storage space managed only by U.S. citizens with government security clearances, Susie Adams, chief technology officer of Microsoft's federal division, said Thursday.

The new suite also should appeal to federal customers because of its tiered pricing model, which runs from $2 to$27 per user per month, Adams said. That will allow agencies to pay a reduced fee for interns and other employees who need access only to a handful of services.

One benefit of being located in the cloud is that providers can upgrade services on a regular basis without having to sell customers new hardware, Adams said. Microsoft plans to roll out upgrades to the cloud-based service every three to six months, she said, but will allow customers to control when the upgrades takes effect so they don't disrupt operations.

Computer clouds essentially are large banks of off-site computer servers that can operate much closer to full capacity than standard servers by rapidly repacking data as one customer surges in usage and another one dips. Cloud customers pay for data storage based on use, as with electricity or another utility, rather than with a set fee.

Federal agencies have historically been hesitant to move their services to the cloud because of security concerns over housing their data off-site.

Adams said she's seen that discomfort ebb in recent years, especially since federal Chief Information Officer Vivek Kundra announced a plan to move roughly one-quarter of the government's information technology budget to the cloud in the next five years.

"People just need to stop and look and make sure you're comfortable that your data and its

sensitivity level matches your cloud provider," Adams said. "There are always going to be security concerns. That's not going to go away. The cloud isn't necessarily more secure or less secure, it's just who has the responsibility [for ensuring its security,] changes [from the agency to the cloud provider]."

Adams speculated agencies will become more comfortable with cloud storage once the government stands up its FedRAMP process, a planned governmentwide certification of private sector IT that will allow it to be adopted by any agency.

The program ran into criticism when it was unveiled in November 2010, because technology companies complained the one-size-fits-all model didn't jibe with the diversity of programs in the federal government. The Obama administration has said it will consider relaxing the requirements and expects to get the program up and running this summer or fall.

Right now, Adams said, many security protocols and security-related operation tweaks have to be worked out on a case-by-case basis between a vendor and a federal agency.

"That's one of the most difficult things for us," she said. "It's time-consuming and very expensive on our end. If you look at the cloud, it's all about economies of scale and when you work with customers on that level of detail on a one-off basis, the whole economies of scale break down. You can't offer each customer a different cloud. That's not really cloud, it's just outsourcing."

*This story has been corrected to reflect the fact that the Agriculture Department, not GSA, granted BPOS Federal Information Security Management Act certification.*

# Dissolution of Hacker Group May Not End Attacks

June 26, 2011

**Dissolution of Hacker Group Might Not End Attacks**
By RIVA RICHMOND and NICK BILTON

Facing increasing pressure from law enforcement agencies over its brazen computer attacks, the small group of hackers known as Lulz Security announced over the weekend that it would disband.

But security experts said on Sunday that the dissolution of the group might not signal an end to the attacks, which have hit dozens of Web sites, including those of prominent targets like the Central Intelligence Agency, the United States Senate, the Arizona state police and Sony.

Indeed, in its farewell message posted on Saturday, the group, also known as LulzSec, urged other hackers to join the "revolution" aimed at governments and corporations that it started recently with Anonymous, a much larger collective of politically minded hackers from which many of the LulzSec members sprung.

"It looks like these sort of 'hacktivist' ideas are spreading and gaining popularity," said Dino A. Dai Zovi, a prominent independent security consultant. He said that LulzSec appeared to be trying to inspire others to join a sprawling, if fragmented, array of local groups, which could feed more attacks.

In recent weeks, LulzSec has become a target itself, as global law enforcement authorities and rival hackers have gone after the group. One man associated with LulzSec, Ryan Cleary, was arrested last week in Britain. Meanwhile, a growing

assemblage of rival hackers has been working to unmask the core half-dozen LulzSec members and feed information on them to the authorities.

American officials on Sunday characterized the attacks carried out by LulzSec as “nuisances” rather than real security threats. One government official said that LulzSec had never penetrated government servers or stolen any classified information.

“What we are really worried about is people getting access to our systems, or putting malware on it,” said the official, speaking on condition of anonymity.

The official said that even though it was possible that LulzSec had disbanded, hackers tended to operate in a world of shifting alliances and it would be easy for a new group copying LulzSec’s techniques to appear in the future.

“All it takes is one guy in his basement to do this, not an organized group,” the official said.

On Monday, the Department of Homeland Security plans to introduce a system to help institutions eliminate common programming errors that allow hackers to easily infiltrate databases and steal user names and passwords. The agency’s hope is that the program, which is voluntary, will make it easier for companies and agencies to better secure their corners of the Internet, thus contributing to a safer global network.

Some security experts and hackers were skeptical of LulzSec’s sudden about-face and said they believed the group intended to continue its activities. The latest announcement could be just another ploy for attention, rival hackers said on Twitter and

on private online message boards.

Over the last several weeks, LulzSec had said repeatedly on its Twitter feed that it planned to continue attacking governments and financial institutions indefinitely.

Members of LulzSec did not respond to phone calls and e-mails on Sunday.

Whatever happens to LulzSec, the brash and public brand of hacking that it embraced and defined may be here to stay, some experts say. The group's attacks on prominent targets, accompanied by raucous bragging on social networks and chat rooms, helped it amass more than 280,000 followers on Twitter. It has used that megaphone, as well as chat rooms, to try to recruit more hackers to its ranks.

Some of LulzSec's activities had a political tinge. For example, it said its theft and public disclosure of Arizona law enforcement records was in response to the state's tough laws aimed at illegal immigrants. But the group claimed that its hacking was primarily a celebration of the "lulz," or laughs, and the members seemed to lap up the media attention they generated.

But if LulzSec had continued, it would have faced an increasing risk that its members would be captured, said Chris Wysopal, the chief technology officer of the security firm Veracode.

"By stopping now and regrouping, I think they will live to hack another day," he said. "If anything, there will be more people hacking in their footsteps."

Mr. Wysopal added, "Until they're arrested — if they ever do get arrested — I don't think

anything will slow down."

The recent flurry of hacking done for notoriety rather than financial gain "feels like a kind of return to a period in the past," said Gabriella Coleman, an assistant professor at New York University who is studying groups like LulzSec and Anonymous.

In the late 1980s and early 1990s, a number of hacker groups brazenly attacked some major institutions. That wave was largely squelched after a crackdown in which well-known hackers, including Kevin Mitnick, were caught and given heavy punishments, Ms. Coleman said.

After that, hackers began working more quietly, and many joined the security industry, where there was a safer place to employ their skills. Meanwhile, organized crime began moving online, following the money that was flowing through Web-based commerce and banking systems.

The return of more public hacking has been inspired by WikiLeaks, whose disclosure of reams of United States government documents showed hackers and the computer adept that they could use their skills to participate in a new way in the public sphere, Ms. Coleman said.

That notion was fed by Anonymous, a large collective of online hackers that opposed the Church of Scientology, championed freedom on the Internet and came to the defense of WikiLeaks by attacking the Web sites of companies like MasterCard and PayPal, which had refused to process donations to WikiLeaks after it disclosed confidential diplomatic cables.

More recently, Anonymous has gotten behind an array of international political causes, from the democratic uprisings in the Middle East to anticorruption protests in India.

LulzSec began as a splinter group from Anonymous, and LulzSec's members now seem to be focusing on operating through that larger network.

To judge from purported discussions between LulzSec members that were posted online by a rival hacker known as the Jester, the internal operations of LulzSec seem as chaotic as the anarchistic behavior online. The messages show continual infighting among group members as pressure from law enforcement agencies has increased, and some members have reportedly quit.

But publicly, LulzSec insisted that its 50 days of online pandemonium had come to an end, its members would continue attacks on governments and corporations, either as part of a different group or acting individually.

Perhaps to win allies, it called the new effort "AntiSec" in an apparent effort to tap an older, similarly named movement among malicious hackers known as "black hats" that opposed working cooperatively with software makers and the security industry to fix security vulnerabilities.

*Mark Mazzetti contributed reporting.*

A Stronger Net Security System Is Deployed

By JOHN MARKOFF
Published: June 24, 2011

“It won’t matter where you are in the world or who you are in the world, you’re going to be able to authenticate everyone and everything,” said Dan Kaminsky, an independent network security researcher who is one of the engineers involved in the project.

The Singapore event included an elaborate technical ceremony to create and then securely store numerical keys that will be kept in three hardened data centers there, in Zurich and in San Jose, Calif. The keys and data centers are working parts of a technology known as Secure DNS, or DNSSEC. DNS refers to the Domain Name System, which is a directory that connects names to numerical Internet addresses. Preliminary work on the security system had been going on for more than a year, but this was the first time the system went into operation, even though it is not quite complete.

The three centers are fortresses made up of five layers of physical, electronic and cryptographic security, making it virtually impossible to tamper with the system. Four layers are active now. The fifth, a physical barrier, is being built inside the data center.

The technology is viewed by many computer security specialists as a ray of hope amid the recent cascade of data thefts, attacks, disruptions and scandals, including break-ins at Citibank, Sony, Lockheed Martin, RSA Security and elsewhere. It allows users to communicate via the Internet with high confidence that the identity of the person or organization they are communicating with is not being spoofed or forged.

Internet engineers like Mr. Kaminsky want to counteract three major deficiencies in today’s Internet. There is no mechanism for ensuring trust, the quality of software is

uneven, and it is difficult to track down bad actors.

One reason for these flaws is that from the 1960s through the 1980s the engineers who designed the network's underlying technology were concerned about reliable, rather than secure, communications. That is starting to change with the introduction of Secure DNS by governments and other organizations.

The event in Singapore capped a process that began more than a year ago and is expected to be complete after 300 so-called top-level domains have been digitally signed, around the end of the year. Before the Singapore event, 70 countries had adopted the technology, and 14 more were added as part of the event. While large countries are generally doing the technical work to include their own domains in the system, the consortium of Internet security specialists is helping smaller countries and organizations with the process.

The United States government was initially divided over the technology. The Department of Homeland Security included the .gov domain early in 2009, while the Department of Commerce initially resisted including the .us domain because some large Internet corporations opposed the deployment of the technology, which is incompatible with some older security protocols.

Internet security specialists said the new security protocol would initially affect Web traffic and e-mail. Most users should be mostly protected by the end of the year, but the effectiveness for a user depends on the participation of the government, Internet providers and organizations and businesses visited online. Eventually the system is expected to have a broad effect on all kinds of communications, including voice calls that travel over the Internet, known as voice-over-Internet protocol.

"In the very long term it will be voice-over-I.P. that will benefit the most," said Bill

Woodcock, research director at the Packet Clearing House, a group based in Berkeley, Calif., that is assisting Icann, the Internet governance organization, in deploying Secure DNS.

Secure DNS makes it possible to make phone calls over the Internet secure from eavesdropping and other kinds of snooping, he said.

Security specialists are hopeful that the new Secure DNS system will enable a global authentication scheme that will be more impenetrable and less expensive than an earlier system of commercial digital certificates that proved vulnerable in a series of prominent compromises.

The first notable case of a compromise of the digital certificates — electronic documents that establish a user's credentials in business or other transactions on the Web — occurred a decade ago when VeriSign, a prominent vendor of the certificates, mistakenly issued two of them to a person who falsely claimed to represent Microsoft.

Last year, the authors of the Stuxnet computer worm that was used to attack the Iranian uranium processing facility at Natanz were able to steal authentic digital certificates from Taiwanese technology companies. The certificates were used to help the worm evade digital defenses intended to block malware.

In March, Comodo, a firm that markets digital certificates, said it had been attacked by a hacker based in Iran who was trying to use the stolen documents to masquerade as companies like Google, Microsoft, Skype and Yahoo.

"At some point the trust gets diluted, and it's just not as good as it used to be," said Rick Lamb, the manager of Icann's Secure DNS program.

The deployment of Secure DNS will significantly lower the cost of adding a layer of

security, making it more likely that services built on the technology will be widely available, according to computer network security specialists. It will also potentially serve as a foundation technology for an ambitious United States government effort begun this spring to create a system to ensure “trusted identities” in cyberspace.

# TDL-4: The 'Indestructible' Botnet

**JUNE 30, 2011 8:15 AM PDT**

**TDL-4: The 'indestructible' botnet?**

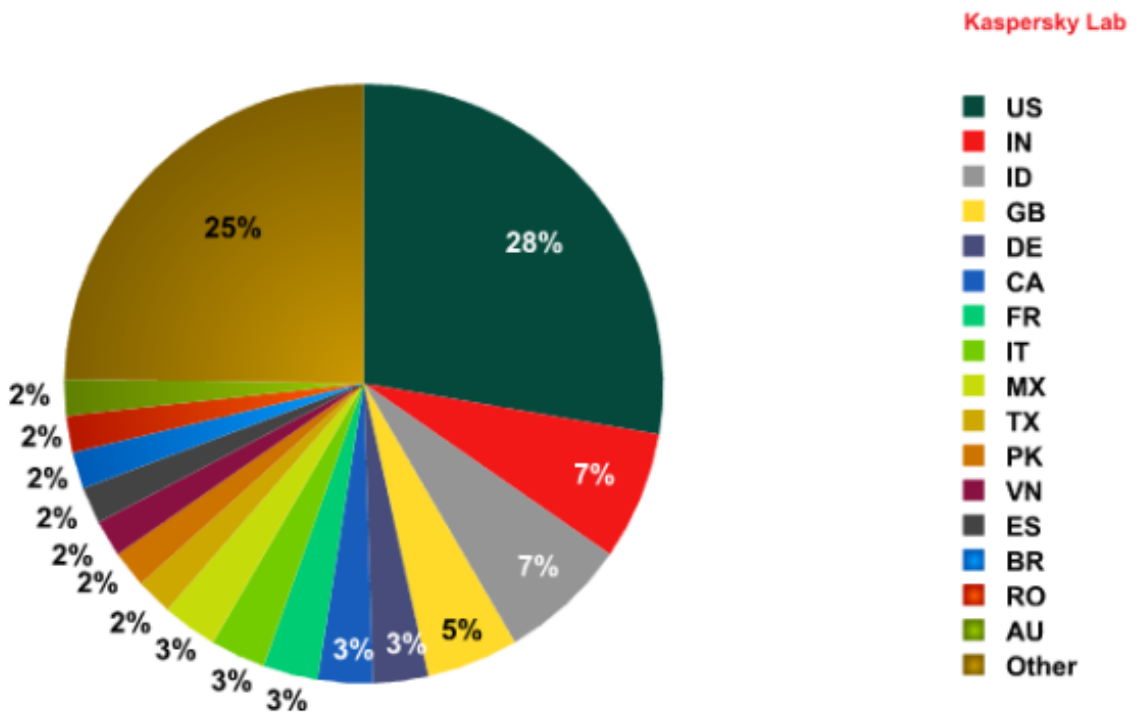
by Don Reisinger

Security researchers at Kaspersky Lab have detailed a new botnet--a collection of infected computers controlled by cybercriminals--called TDL-4, that might just be "indestructible."

TDL-4 gets its name by being the fourth generation of the botnet. In 2008, the original TDL appeared. It has been altered over the last several years. With TDL-4, Kaspersky has found, the malware creators have drastically improved the botnet over its predecessors.

"The malware writers extended the program functionality, changed the algorithm used to encrypt the communication protocol between bots and the botnet command and control servers, and attempted to ensure they had access to infected computers even in cases where the botnet control centers are shut down," Kaspersky wrote on its SecureList blog earlier this week. "The owners of TDL are essentially trying to create an 'indestructible' botnet that is protected against attacks, competitors, and antivirus companies."

Central to TDL-4's updates is an improved algorithm that encrypts communications between infected computers and the botnet's command. According to Kaspersky, TDL-4 creates an identifier known as "bsh parameter" that "acts as one of the encryption keys for subsequent connections to the command and control server." Once a request between command and the computer is activated, it's transmitted over an HTTPS connection. According to Kaspersky, that system helps the botnet "run smoothly" and, at the same time, stops anyone else from trying to take control over it.




Global distribution of TDL-4 infections. According to the country codes to the right, the U.S., India, Indonesia, and Great Britain are tops in infections, according to Kaspersky. (Credit: Kaspersky Lab)

To help safeguard itself from removal, TDL-4 infects a computer's master boot record, thus allowing it to run before the operating system starts up, and keep it away from the prying eyes of anti-malware programs. What's more, the botnet deletes other malicious files that might get caught by security tools and tip users to TDL-4 running on their computers. In their place, TDL-4 has downloaded about 30 malicious programs on infected computers, including "fake anti-virus programs, adware, and the Pushdo spambot," Kaspersky says.

According to Kaspersky, the botnet also uses peer-to-peer network Kad to issue several commands, including searching for new files, publishing files to Kad, and more.

The big upshot of that for TDL-4 creators, Kaspersky says, is that even if "its command and control centers are shut down, the botnet owners will not lose control over infected machines," since they'll still be able to access Kad.

Although Kaspersky believes TDL-4 is practically impenetrable, not everyone is so quick to agree. Writing for InfoWorld today, Roger Grimes, a self-described "24-year veteran of the malware wars," says that there has yet to be a single threat that has

been able to hold its ground indefinitely.

"I can safely tell you that no threat has appeared that the antimalware industry and OS vendors did not successfully respond to," Grimes writes. "It may take months or years to kill off something, but eventually the good guys get it right."

He makes a solid point. Last year, Conficker was taken down after wreaking havoc on computers worldwide since 2008. Earlier this month, the FBI announced that it had taken down the Coreflood botnet.

But TDL-4's functionality might just be in a league of its own. As Kaspersky notes, the botnet can "manipulate adware and search engines, provide anonymous Internet access, and act as a launch pad for other malware."

According to Kaspersky, 28 percent of all infected TDL-4 computers are in the U.S. Computers in the U.K., Italy, France, and many other countries are also infected with TDL-4. All told, more than 4.5 million computers were infected with TDL-4 in the first three months of 2011 alone.

# Security Researchers Discover 'Indestructible" Botnet

**30 June 2011** Last updated at 06:34 ET

### Security researchers discover 'indestructible' botnet

Cracking the TDL-4 botnet is going to be hard, say security experts.

**More than four million PCs have been enrolled in a botnet security experts say is almost "indestructible".**

The botnet, known as TDL, targets Windows PCs and is difficult to detect and shut down.

Code that hijacks a PC hides in places security software rarely looks and the botnet is controlled using custom-made encryption.

Security researchers said recent botnet shutdowns had made TDL's controllers harden it against investigation.

The 4.5 million PCs have become victims over the last three months following the appearance of the fourth version of the TDL virus.

The changes introduced in TDL-4 made it the "most sophisticated threat today," **wrote Kaspersky Labs security researchers Sergey Golovanov and Igor Soumenkov in a detailed analysis of the virus.**

"The owners of TDL are essentially trying to create an 'indestructible' botnet that is protected against attacks, competitors, and anti-virus companies," wrote the researchers.

Recent successes by security companies and law enforcement against botnets have **led to spam levels dropping to about 75% of all e-mail sent**, shows analysis by Symantec.

# Security Researchers Discover 'Indestructible" Botnet

A botnet is a network of computers that have been infected by a virus that allows a hi-tech criminal to use them remotely. Often botnet controllers steal data from victims' PCs or use the machines to send out spam or carry out other attacks.

The TDL virus spreads via booby-trapped websites and infects a machine by exploiting unpatched vulnerabilities. The virus has been found lurking on sites offering porn and pirated movies as well as those that let people store video and image files.

**It's definitely one of the most sophisticated botnets out there”**

Joe Stewart

The virus installs itself in a system file known as the master boot record. This holds the list of instructions to get a computer started and is a good place to hide because it is rarely scanned by standard anti-virus programs.

The biggest proportion of victims, 28%, are in the US but significant numbers are in India (7%) and the UK (5%). Smaller numbers, 3%, are found in France, Germany and Canada.

However, wrote the researchers, it is the way the botnet operates that makes it so hard to tackle and shut down.

The makers of TDL-4 have cooked up their own encryption system to protect communication between those controlling the botnet. This makes it hard to do any significant analysis of traffic between hijacked PCs and the botnet's controllers.

In addition, TDL-4 sends out instructions to infected machines using a public peer-to-peer network rather than centralised command systems. This foils analysis because it removes the need for command servers that regularly communicate with infected machines.

"For all intents and purposes, [TDL-4] is very tough to remove," **said Joe Stewart, director of malware research at Dell SecureWorks to Computerworld.** "It's definitely

one of the most sophisticated botnets out there."

However, the sophistication of TDL-4 might aid in its downfall, said the Kaspersky researchers who found bugs in the complex code. This let them pry on databases logging how many infections TDL-4 had racked up and was aiding their investigation into its creators.

## A Smarter, Stealthier Botnet

*The "most technologically sophisticated" malware uses clever communications tricks and encryption to avoid disruption.*

- FRIDAY, JULY 1, 2011
- BY DAVID TALBOT

A new kind of botnet—a network of malware-infected PCs—behaves less like an army and more like a decentralized terrorist network, experts say. It can survive decapitation strikes, evade conventional defenses, and even wipe out competing criminal networks.

The botnet's resilience is due to a super-sophisticated piece of malicious software known as TDL-4, which in the first three months of 2011 infected more than 4.5 million computers around the world, about a third of them in the United States.

The emergence of TDL-4 shows that the business of installing malicious code on PCs is thriving. Such code is used to conduct spam campaigns and various forms of theft and fraud, such as siphoning off passwords and other sensitive data. It's also been used in the billion-dollar epidemic of fake anti-virus scams.

"Ultimately TDL-4 is simply a tool for maintaining and protecting a compromised platform for fraud," says Eric Howes, malware analyst for GFI Software, a security company. "It's part of the black service economy for malware, which has matured considerably over the past five years and which really needs a lot more light shed on it."

Unlike other botnets, the TDL-4 network doesn't rely on a few central "command-and-control" servers to pass along instructions and updates to all the infected computers. Instead, computers infected with TDL-4 pass along instructions to one another using

public peer-to-peer networks. This makes it a "decentralized, server-less botnet," wrote Sergey Golovanov, a malware researcher at the Moscow-based security company Kaspersky Lab, on this blog describing the new threat.

"The owners of TDL are essentially trying to create an 'indestructible' botnet that is protected against attacks, competitors, and antivirus companies," Golovanov wrote. He added that it "is one of the most technologically sophisticated, and most complex-to-analyze malware."

The TDL-4 botnet also breaks new ground by using an encryption algorithm that hides its communications from traffic-analysis tools. This is an apparent response to efforts by researchers to discover infected machines and disable botnets by monitoring their communication patterns, rather than simply identifying the presence of the malicious code.

Demonstrating that there is no honor among malicious software writers, TDL-4 scans for and deletes 20 of the most common forms of competing malware, so it can keep infected machines all to itself. "It's interesting to mention that the features are generally oriented toward achieving perfect stealth, resilience, and getting rid of 'competitor' malware," says Costin Raiu, another malware researcher at Kaspersky.

Distributed by criminal freelancers called affiliates, who get paid between $20 and $200 for every 1,000 infected machines, TDL-4 lurks on porn sites and some video and file-storage services, among other places, where it can be automatically installed using vulnerabilities in a victim's browser or operating system.

Once TDL-4 infects a computer, it downloads and installs as many as 30 pieces of other malicious software—including spam-sending bots and password-stealing programs. "There are other malware-writing groups out there, but the gang behind [this

one] is specifically targeted on delivering high-tech malware for profit," says Raiu.

# A 'Futures' Market for Computer Security

Tuesday, July 5, 2011

**A Futures Market for Computer Security**

A predictions market could help companies prepare for major security incidents before they happen.

By Brian Krebs

Information security researchers from academia, industry, and the U.S. intelligence community are collaborating to build a pilot "prediction market" capable of anticipating major information security events before they occur.

A prediction market is similar to a regular stock exchange, except the "stocks" are simple statements that the exchange's members are encouraged to evaluate. Traders will buy and sell "shares" of a stock based on the strength of their confidence about the future outcome—with an overall goal of increasing the value of their portfolios, which will in turn earn them some sort of financial reward. Traders may choose to buy or sell additional shares of a stock, and that buying and selling activity pushes the stock price up or down, just as in a real market.

Some of the stocks being considering cover a few months, such as: "The volume of spam e-mail will increase by 10 percent in the third quarter of 2011." Others will ask participants to gauge the likelihood of far-off events, such as the chance that the U.S. House of Representatives will pass a bill with "cyber" and "security" in its title in the first session of the 112th Congress, or whether broadly used encryption algorithms will be defeated within the next 24 months.

Greg Shannon, chief scientist of the CERT program at Carnegie Mellon's Software Engineering Institute, who is involved with the project, says the purpose is to provide actionable data.

"If you're Verizon, and you're trying to pre-position resources, you might want to have some visibility over the horizon about the projected prevalence of mobile malware," Shannon said. "That's something they'd like to have an informed opinion about by leveraging the wisdom of the security community."

Predictions markets have effectively forecasted all manner of events and trends, from the success of sports teams to the sales of new products. The pilot project will rely on software and services provided by Consensus Point, a Nashville-based company that

has helped to build employee-driven prediction markets for several major companies, including General Electric, Best Buy, and Qualcomm. Best Buy's prediction market—called "TagTrade"—is designed to give management an early indicator of which new products or ideas are likely to succeed, and whether specific new stores will open on time.

The University of Iowa's Iowa Electronic Markets, one of the earliest prediction markets, has significantly outperformed the polls in every presidential election when forecasting more than 100 days in advance: Compared to 964 polls over the five presidential elections since 1988, the Iowa market was closer to the eventual outcome 74 percent of the time. The University of Iowa also uses prediction markets to forecast seasonal flu outbreaks.

Prediction markets have a major built-in bias—those answering the questions are not polled randomly—but respondents also have an incentive to respond only to those questions they feel confident in answering with accuracy.

"Prediction markets aren't just surveys that ask everyone to speak up," Robin Hanson, chief scientist at Consensus Point. " People tend to speak up only when they're reasonably sure they know the answer."

Consensus Point CEO Linda Rebrovick says the goal of the project is to attract a network of about 250 experts, although the organizers are still deciding how to compensate for correct answers.

"There will be some combination of rewards and financial incentives for participating," Rebrovick says.

Even if questions generate only tepid responses, such responses can be informative, says Dan Geer, chief information security officer at In-Q-Tel, the venture capital arm of the Central Intelligence Agency (CIA). Geer is also involved in the project. "It may be that this tells us there is ambiguity, or that we are, in effect, measuring disagreement on a question that doesn't have a quantitative aspect to it," Geer says. "Straight-out surveys are vulnerable to idiot answers, and prediction markets are vulnerable to stupid questions."

While the pilot project will be limited to invited information security experts, the consensus decisions reached by the group will be made public. "Even if we can't find something useful in all of this, we feel that's a valuable result. It's the way you make

progress," Geer says.

# Former CIA Director: Build a New Internet to Improve Cybersecurity

## Former CIA Director: Build a new Internet to improve cybersecurity

BY ALIYA STERNSTEIN 07/06/2011

The United States may seriously want to consider creating a new Internet infrastructure to reduce the threat of cyberattacks, said Michael Hayden, President George W. Bush's CIA director.

Several current federal officials, including U.S. Cyber Command chief Gen. Keith Alexander, also have floated the concept of a ".secure" network for critical services such as banking that would be walled off from the public Web. Unlike .com, .xxx and other new domains now proliferating the Internet, .secure would require visitors to use certified credentials for entry and would do away with users' Fourth Amendment rights to privacy. Network operators in the financial sector, for example, would be authorized to scan account holders' traffic content for signs of trouble. The current Internet setup would remain intact for people who prefer to stay anonymous on the Web.

"I think what Keith is trying to suggest is that we need a more hardened enterprise structure for some activities and we need to go build it," Hayden said during a roundtable on cybersecurity hosted by the Potomac Institute for Policy Studies. "All those people who want to violate their privacy on Facebook -- let them continue to play."

Nations with fewer civil liberty protections, including China, use "deep packet inspection" to search all Internet traffic for viruses -- as well as anti-government content, noted James Mulvenon, a China and cybersecurity specialist. Due to privacy laws, the United States cannot monitor private network traffic using this approach. Mulvenon questioned whether such restrictions give other nation states the upper hand in cyber defense. "We still believe that anonymity is possible," he said of America's attitude toward freedom of expression on the Internet.

Mulvenon, an executive at Defense Group Inc., a government contractor that provides agencies with intelligence analysis, has in mind a three-level network. "If you want to do banking, there's no anonymity," and users would need to enter true names and digital credentials to operate in the space, he said. The middle level, perhaps applicable to the .edu domain, would require fewer personal details from visitors.

"At the bottom, you can run around like a hobbit," he said. "How can you have a multilevel system that allows you to play up here and down there and doesn't compromise your ability to play?" is the challenge.

Sen. Sheldon Whitehouse, D-R.I., chairman of the Judiciary Crime and Terrorism subcommittee, has cited Alexander's backing of the idea to urge that his fellow lawmakers help create a .secure

domain.

"This doesn't have to be complicated or even mandatory," he said on the Senate floor in November 2010. "The most important value of a dot-secure domain is that, like dot-gov and dot-mil, now we can satisfy consent under the Fourth Amendment search requirements for the government's defenses to do their work within that domain, their work of screening for attack signals, botnets and viruses."

Today, searches of the .gov domain are conducted by the Einstein program, an intrusion prevention and detection system under the direction of the Homeland Security Department that monitors only federal traffic for signs of unauthorized access. It alerts response teams to potential attacks and automatically blocks penetration in some cases.

Whitehouse went on to say, "Core elements of our electric grid, of our financial, transportation and communications infrastructure would be obvious candidates. But we simply cannot leave that core infrastructure on which the life and death of Americans depends without better security."

The Obama administration and lawmakers currently are collaborating on sweeping cybersecurity legislation to bolster federal oversight of commercial and civilian government networks. The White House's proposal would not physically segregate critical infrastructure networks but would place those systems under greater DHS oversight.

# Threat of Destructive Coding in Foreign-Manufactured Technology Is Real

## Threat of destructive coding on foreign-manufactured technology is real

BY ALIYA STERNSTEIN 07/07/2011

The federal government has identified technology components in the U.S. supply chain that have been embedded with security flaws, the top U.S. civilian cybersecurity official said Thursday.

Greg Schaffer, acting deputy undersecretary of the Homeland Security Department National Protection and Programs Directorate, confirmed the threat during a House Oversight and Government Reform Committee hearing on cybersecurity. At the time of a January federal report on the U.S-China supply chain, conversations had been largely hypothetical about "backdoor" mechanisms, where outsiders insert faulty programming into foreign-manufactured devices to, for example, shut down systems remotely or leak information.

"These pieces are embedded in software and hardware and people don't know that. It's very difficult to detect," said Rep. Jason Chaffetz, R-Utah, chairman of the Subcommittee on National Security, Homeland Defense and Foreign Operations. "Are you aware of any software or hardware components that have been embedded with security risks?" he asked Schaffer.

At first, the DHS official hesitated to provide a yes or no answer, but after repeated questioning, he replied, "I am aware that there have been instances where that has happened."

The revelation follows many congressional hearings on the growing fear that nation states and rogue criminals are undermining the U.S. economy by hacking into proprietary data and other sensitive information. This spring, the White House released an international strategy and legislative proposal to bolster network security.

"To date, public discussion of the vulnerabilities of electronics components to malicious tampering has been largely theoretical," the January U.S.-China Economic and Security Review Commission staff report stated. It said "kill switches" could be installed in Pentagon systems to power down operations in response to remote commands. "The potential for harm is enormous, extending from simple identity theft by criminal enterprises to disrupting networks and defense systems vital to national security," the commission wrote.

The international cybersecurity strategy notes the federal government reserves the right to use military force in response to certain hostile acts in cyberspace. Lawmakers on Thursday asked witnesses to specify when a cyber incident would qualify as this type of hostile act.

James A. Baker, U.S. associate deputy attorney general, said the question is legally difficult to answer but "acts [in cyberspace] that would be equivalent . . . to kinetic attacks on the Unites

States" would constitute an "act of war."

Even with a legal determination that war is under way, the U.S. military would still have to conduct "a fairly complicated forensic analysis" to identify an adversary, said Robert J. Butler, Defense deputy assistance secretary for cyber policy.

The White House legislative proposal would mandate that all agencies continuously monitor federal computer equipment and software with automated tools to spot threats faster. Current law requires agencies to fill out paperwork to confirm compliance with security safeguards only once a year.

Members on Thursday wanted to know the price tag for deploying real-time surveillance. Officials from Homeland Security, which is in charge of governmentwide cyber operations, could not provide a cost analysis but agreed to work with Congress on budgeting expenditures into legislation.

"We recognize that much of the work and effort and spending that is done today [for] compliance, check-the-box activities, can be repurposed . . . that allows us to actually buy down risk," Schaffer said. Over the long run, "the expense associated with all the work we do to chase the problems will be reduced . . . Building it in is much cheaper that bolting it on.

# Symantec Compares iOS and Android Security

Symantec compares iOS and Android security

by Mikael Ricknäs, IDG-News-Service:Stockholm-Bureau Jun 28, 2011 11:40 am

Apple's iOS and Google's Android smartphone platforms are more secure than traditional desktop-based operating systems, but are still susceptible to many existing categories of attacks, according toa 23-page report from security software vendor Symantec.

The good news is that Apple and Google designed their respective operating systems with security in mind. But keeping up with a constantly changing threat landscape is difficult. In the report, "A window into mobile device security," Symantec evaluated the two operating systems for how they stood up to Web-based and network-based attacks, social engineering attacks, attacks on the integrity of the device's data, and malware.

Users of both Android and iOS smartphones and tablets regularly synchronize their devices with cloud services and with their home desktop computers. This can potentially expose sensitive enterprise data to systems outside the control of the enterprise, according to Symantec.

When it comes to protecting against traditional malware, Apple's certification of applications and developers protects users, according to Symantec. On the other hand, Google's less rigorous certification mode has arguably led to today's increasing volume of Android-specific malware, the company said. Earlier this month Google had to remove yet more malware-infected apps offered in its Android Market.

Google's more open approach has been one of the reasons for its success, according to Ben Wood, director of research at CCS Insight. It has helped Google to quickly increase

the number of available applications. So far, the offending apps haven't had a major affect on users, but user sentiment could change quickly if they are hit by more severe attacks, Wood said.

As has been pointed out by security experts in the past, Android's reliance upon the user to grant a set of permissions is a weak link. A majority of users are simply not technically equipped to make these security decisions. In contrast, Apple's iOS platform simply denies access, under all circumstances, to many of the device's more sensitive subsystems, according to Symantec. On Android, a malicious app simply requests the set of permissions it needs to operate, and in most cases, users happily grant these permissions.

On the plus side, Google does require that developers pay a fee and register with the company to be able to distribute their apps via the official Android App Marketplace, Symantec said.

Possible weaknesses in iOS include its encryption, according to Symantec. The majority of the data is encrypted in such a manner that it can be decrypted without the need for the user to input the device's master passcode. This means that an attacker with physical access to an iOS device can potentially read most of the device's data without knowing the passcode, Symantec said. In February, researchers in Germany showed how they could do this in six minutes on an iPhone running iOS 4.2.1, Symantec warned.

Also, attacks against specific applications like the iOS Web browser, while being self-contained and blocked from impacting other apps, can still cause significant harm to a device.

Android recently began offering built-in encryption in Android 3.0. However, earlier versions of Android, which are running on virtually all mobile phones in the field, contain no encryption capability.

# Symantec Compares iOS and Android Security

So far, security researchers have uncovered about 200 different vulnerabilities in various versions of iOS. But the vast majority of these vulnerabilities have been of a lower severity. To date, all but four of the 18 vulnerabilities on Android have been patched by Google. One has been fixed in version 2.3, but it has not been fixed for prior versions of the operating system. For example, the recent Android.Rootcager, also known as Android.DroidDream, and Android.Bgserv threats both leveraged this vulnerability to obtain administrator-level control, according to Symantec.

Symantec also has a word of warning for users with jailbroken smartphones. They are an attractive target for attackers since they are every bit as vulnerable as traditional PCs, it said.

Symantec concluded that iOS offers better access control, application provenance and encryption. Google's Android offers better application isolation, and the permission-based access control category is a tie, according to Symantec. Apple also offers better protection against malware attacks, service attacks, data loss and data integrity attacks. Both offer full protection against Web attacks, and no protection technologies to address social engineering attacks such as phishing or spam.

Security on smartphones is a growing challenge that vendors need to address, according to Wood. Large-scale attacks can end up having a detrimental effect on smartphone popularity, he said.

attacks are going after military secrets without any fear of retaliation, he said.

## U.S. Military Expanding Arsenal of Cyber-Warfare Capabilities

By: Fahmida Y. Rashid

2011-06-23

The federal government is increasingly using cyber-tactics to defend its IT assets against attackers and to protect its interests. It's about time, since enemies are already relying on an extensive arsenal of cyber-weapons, experts said.

President Obama has signed executive orders outlining how far the United States military can go when launching cyber-attacks and other cyber-operations against enemies and as part of routine espionage activities, the Associated Press reported June 22.

The orders, which were signed more than a month ago and cap a two-year Pentagon effort to draft rules for the U.S. military, detail when the military needs to seek presidential approval for a specific cyber-assault and how the Department of Defense will integrate cyber-capabilities into military strategy, defense officials said.

The strategy document outlines some of the approved activities, such as planting a computer virus on adversaries' computers to launching attacks that bring down a target electrical grid or defense network. When under attack, the United States can defend itself by blocking cyber-intrusions and taking down servers in another country. And similar to a missile attack, the military can pursue attackers across national boundaries, the AP reported.

"We must have the capability to defend against the full range of cyber-attacks," Deputy Defense Secretary William Lynn said. Terror groups will eventually learn how to launch crippling cyber-attacks, so the United States needs to be more aggressive in offensive and defensive countermeasures, he said.

Many of the attacks on American businesses, critical infrastructure and defense systems are a "direct challenge" to our military superiority, Charles Dodd, a government consultant for cyber-defense and an adviser to the House of Representatives Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, told eWEEK. State-sponsored

"We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests," the policy said. Military force would be used only after all other options have been exhausted.

The Pentagon has also developed a list of cyber-weapons and tools, including viruses that can sabotage foreign critical infrastructure, that the United States can use "to deter or deny a potential adversary the ability to use its computer systems," an anonymous official recently told the Washington Post.

The techniques to launch a cyber-attack are similar to those of any other military operation, according to Dodd. Extensive reconnaissance, surveillance and research are required before launching a cyber-attack, he said. The executive orders apparently allow the military to transmit code to another country's network to test the route and make sure connections work, much like using satellites to take pictures of a location to scout out specific sites.

Elsewhere on Capitol Hill, government officials have been discussing how to protect critical infrastructure. The federal government is considering creating a separate Internet domain for private-sector critical infrastructure, one that would be subject to monitoring by the government for cyber-threats, Ari Schwartz, Internet policy adviser at the National Institute of Standards and Technology, said before a panel of the Senate Judiciary Crime and Terrorism subcommittee on June 21.

The panel's chairman, Sen. Sheldon Whitehouse, D-R.I., has long supported the creation of a .secure domain, arguing that the government would be able to closely monitor Internet traffic without violating the Fourth Amendment. "You just say, 'OK, look, if you want to go look at these electrical grid things, you've got to be aware that the government is going to be keeping an eye of what's going in and out of there to protect the electrical grid.' I don't think people mind that," Whitehouse said.

Attackers can easily "prove a point" by taking out critical infrastructure, Dodd said.

Whitehouse also said publicly traded companies should be required to disclose their cyber-security risks in Securities and Exchange Commission filings. There is no point in promoting cyber-security awareness if actual attacks are classified if they hit .gov and .mil domains and are treated as proprietary information when businesses are hit so as not to alarm customers,

Whitehouse said, calling it a "real information deficit."

## Lessons from Estonia: Preparing for a major cyberattack

BY ERIN DIAN DUMBACHER 07/06/2011

In the spring of 2007, Estonia became the first nation to face a coordinated, nationwide cyberattack when a series of electronic bombardments struck down media, telecommunications, government and banking websites. Digital traffic from servers as far away as Peru, Vietnam and the United States flooded Estonian websites, drowning them in superfluous data. The attack knocked telephone exchanges offline for more than an hour, jeopardizing emergency services. It knocked out media and government portals, leaving citizens in an information vacuum. Beginning April 29, three waves of attacks during a two week period severely disrupted the ordinary tasks that fuel modern economies -- shopping, pumping gas, withdrawing cash from automatic teller machines. A significant act of cyberterrorism posed an economic and political threat in a way no modern economy had previously experienced.

The onslaught against Estonian websites began after two days of rioting in the capital, Tallinn, spurred by the government's removal of a Soviet-era statue honoring deaths in World War II. By the time officials cleared the streets of shattered glass and protesters, the dispute had moved online.

Though primitive by today's standards, the distributed denial-of-service attacks on Estonia highlighted the central dilemma of online attacks -- attributing the assault to the individuals or governments behind them. While attribution is elusive -- skilled attackers typically hijack foreign servers to perpetrate their crimes -- it is widely believed that Russia funded and led the execution of the attacks against its western neighbor. The architecture of the Internet allowed networks of bots, called botnets, to direct millions of packets to the servers of the Estonian targets, overloading and rendering them inaccessible to visitors.

"It's a new form of public-private partnership," warned Estonian President Toomas Hendrik Ilves in an April interview with *Nextgov*. "It requires massive numbers of computers. There are organized crime rings and they do this by length of time, but you have to have someone willing to pay for it -- that's where the public side of the public-private partnership comes in."

Had the small Baltic nation not been one of the most wired countries in the world, such an attack might have been a blip on the screen of public awareness. In the two decades since breaking away from the former Soviet Union, Estonia built its new democratic society around Web-based services. Estonians were among the first to conduct elections online and today they perform 98 percent of their banking online. For the nation that spawned the global telecommunications phenomenon known as Skype, the 2007 attacks were a watershed moment. Estonia's experience and subsequent actions continue to offer lessons for security managers who face more advanced

threats today.

**Professional networks are critical**

The informal relationships among technology professionals built through old-fashioned networking were key to government and private sector responses to the crisis in 2007. Estonia's two-person computer emergency response team recruited help, calling on national and foreign experts. Swedes and Americans especially aided the response efforts by halting Internet traffic before it reached Estonia. The government also turned to the local, private specialists who had helped set up the country's electronic-voting security system.

The professional network of technologists is small, yet formal mechanisms for quick and effective coordination did not exist. Estonian officials are now establishing policies and procedures to activate this network as needed and have recruited a volunteer army of IT professionals from public and private organizations -- a National Guard for cyberdefense. Volunteers train on weekends for emergencies, while employers gain a more experienced workforce. Internationally, Estonia advocates for more stringent cybercrime regimes and clear cybersecurity policies among NATO allies. What is the lesson for U.S. leadership? Use meaningful, project-based collaboration to connect with colleagues across agencies and in the private sector.

**Go beyond 'partnership'**

Infiltrators do not respect national borders or distinctions between public and private infrastructure. An adequate response to a cyberattack requires coordination among various organizations and individuals in the government and the private sector.

Working with the private sector in Estonia required more than just regulation. While regulators encouraged private sector feedback and information sharing, officials found that cooperation needed to be institutionalized; voluntary associations were insufficient to create the kinds of relationships necessary to coordinate an effective cyber response. Large organizations had the resources to maintain their own systems; small and medium-size enterprises were vulnerable. All needed incentives to share the details of their breaches.

The challenge is global because the networks are global. While NATO and other international bodies are recognizing and acting on the need for more effective partnerships, "I think where we really need to do work is redefining the boundaries between the government [and the] private sector," Ilves said.

**Acknowledge the international dimension**

Today, the centerpiece of Estonia's cybersecurity strategy is engagement with foreign partners' networks and intelligence operations. Estonia has consciously enhanced its partnership with the FBI and it played a central role in standing up the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, which stages attack scenarios and encourages members to share best practices. Linnar Viik, Estonia's technology guru, is a regular participant in cyber-related efforts by the United Nations and the Estonian government advocates signatories to the Council of Europe Convention on Cybercrime. The United States signed on in 2006 and most European countries have joined. Russia and China have not.

**Get ahead of the threat**

Without official processes in 2007, Estonian site managers first tried the "whack-a-mole" approach, trying to defeat each wave of traffic separately. As the onslaught continued and the origins of the traffic came from a diverse set of servers around the world, managers shut off all inflow from abroad. The liberty to shut off all foreign traffic is one the U.S. does not have; restricting access could severely damage the global economy.

The Obama administration has been consumed with a series of economic and political crises since taking office, with the whack-a-mole moniker attributed to its policy in the Middle East, the economy and more. Estonian policymakers had the benefit of a crisis to form a comprehensive strategy and to advise the public how to prepare for and retaliate against upcoming attacks. U.S. private and public networks cannot afford to be unprepared.

# Navy Cyber Unit Scans Horizon For New Challenges

## Navy's cyber unit scans horizon for new challenges

***Fleet Cyber Command takes stock of situational awareness capabilities, reviews operational structure***

- By Amber CorrinJun 21, 2011

In a little more than a year, the Navy's Fleet Cyber Command/10th Fleet has grown from an operations center with only two visualization centers to a hub of situational awareness for the military service.

The Navy activated the Fleet Cyber Command in January 2010 as the service's segment of the joint Cyber Command, and it simultaneously recommissioned the 10th Fleet to handle the Navy's cyber operations worldwide. A year into its existence, the Fleet Cyber Command/10th Fleet is looking toward its future, beginning with a full assessment of its structure and operations, according to its commander, Vice Adm. Bernard "Barry" McCullough.

“A year ago when we started, we had very little situational awareness of the network, and our ability to identify our command and control networks was challenged,” McCullough said. “As we’ve evolved, we’re starting to review whether our organization is 100 percent right or whether we need to restructure along the lines of operation.”

As commander of the Fleet Cyber Command/10th Fleet, McCullough can establish, direct and execute Navy cyberspace operations around the world. After its creation, the unit's first goal was to establish situational awareness for Navy networks, McCullough said. Early in its existence, the command went through a major exercise at Pacific Command to determine what data the Navy needed to visualize the status of its networks and assets and how to clearly display that information, he said.

“Now we have network defense situational awareness, health of transport situational awareness, force geolocation situational awareness and collection situational awareness," McCullough said. "We have built all of that into our current operational picture.”

Because the Navy strives for information dominance over its adversaries, the ability to visualize data for quick analysis is vital to cyberspace operations, said Vice Adm. William Leigher, deputy commander of the Fleet Cyber Command/10th Fleet.

“It’s not that we have too much information — we need a different way of looking at the information available to us,” Leigher said earlier this year. “We need to broaden the role of information and deepen our understanding. And we need experience operating in contested environments; we need training.”

In an effort to better harness information for improved command and control, the Navy’s cyber unit is focusing on regional aspects of the global network, McCullough said. To do so, the 10th Fleet is developing regional network operations and subordinate security commands, he said.

Training and education also are top priorities now that the Fleet Cyber Command/10th Fleet has established situational awareness, McCullough said. To hone cyber skills, the Navy will start broad training, followed by more narrow education at a graduate level. That effort will begin this summer with a new training program that will incorporate student feedback.

“One concern is how to do servicewide training for the entire Navy, including contractors,” McCullough said. “We want to make sure we’ve got total service training at the right level.”

A year after its initial launch, the Fleet Cyber Command/10th Fleet is shifting focus to other tasks while still working on a situational awareness picture that is constantly evolving. Some of those tasks include taking on the ever-present network security challenge, getting the right operational alignment in place and dealing with the cultural issues inherent to all major operational changes, McCullough said.

He added that so far, he’s encouraged by the progress made since the command’s creation last year.

“We’ve come a long way,” McCullough said. "We have achieved what we set out to achieve a year ago. Now the biggest challenge is to maintain the momentum and keep

evolving.”

**Navy Vows to Fight for Its Superlaser, Hypersonic Gun**

- By Spencer Ackerman and Noah Shachtman June 24, 2011 | 9:00 am | Categories: Lasers and Ray Guns **@dangerroom** · 20.2K followers

Rear Adm. Nevin Carr is the Chief of Naval Research, in charge of hundreds and hundreds of different R&D programs — about 3 billion dollars' worth of science projects, next-gen gadgets, and upgrades to the Navy arsenal. But of all those many efforts, there are two that get Carr really pumped: a superlaser and a hypersonic gun. Both are capable of revolutionizing how the Navy fights at sea. Both are considered "marquee" programs by Carr as his legion of scientists and engineers.

And both of them are on the precipice of destruction from Congress.

Lawmakers have traditionally left military research budgets intact, tinkering at the margins only when they feel money is being seriously misspent or the R&D projects are seriously off-track. Rarely, if ever, do they go after a service's top research priority.

Last Friday, however, the Senate Armed Services Committee broke with tradition, and declared that Carr's babies, the Free Electron Laser and the Electromagnetic Railgun, weren't fit to grow up any more. The panel said funds for the programs should be terminated.

Neither project was in trouble — in fact, both had recently broken records in their respective fields. But in Washington's new atmosphere of austerity, the ray gun and the railgun were suddenly considered futuristic luxuries, not the "game-changers" Carr had touted for so long.

The recommended recommended cuts took the Navy by surprise, according to ace naval reporter Sam LaGrone at *Jane's*. Carr's shop has said nothing since then, referring all questions to Big Navy.

Big Navy, at least, isn't throwing in the towel.

"The programs were part of the president's budget and we hope to see them in the final bill," says Lt. Cmdr. Justin Cole, a Navy spokesman. "We will continue to work with Congress to answer any questions they may have about the programs in an effort to secure authorization and funding for their continuation."

But the strongest advocate for both the Free Electron Laser and the railgun has been

Carr himself. He told Danger Room in February that technology had basically maxed out the possibilities for hitting "maneuvering pieces of metal in the sky with other maneuvering pieces of metal."

The solution, as Carr sees it, is hypersonic guns and multi-wavelength lasers. They'd allow the Navy's surface ships to fire at targets from hundreds of miles away and burn incoming missiles out of the sky. For the Senate panel to put them on the chopping block is to ask the Navy to rewrite what it considers the future of surface-ship defense.

Consider the railgun, for instance. When it gets up to its full energy allotment of 64 kilojoules, it'll fire a bullet 200 nautical miles in six minutes. The five-inch guns on destroyers? 13 miles. The 57-mm guns on the Littoral Combat Ship? Seven to eight. BAE's Advanced Gun System, still in development, tops out at 83 nautical miles.

"enduring requirement for fire support from naval vessels in the range of 41-63 nautical miles." (.pdf) Anything that would reduce the ranges of Navy guns would be "something of concern."

As for the Free Electron Laser, the Senate panel doesn't recommend terminating the Navy's entire laser programs — just the "marquee." Unlike other lasers, the Free Electron Laser operates on multiple wavelengths, so as to minimize interference from all the crud in sea air. "The ability to tune even a little bit would allow us to find favorable wavelengths in the atmosphere and then optimize the beam for the conditions of the day," Carr said. "That's very, very powerful."

"You're beginning, maybe, to see the end of the dominance of the missile," Carr's boss, Chief of Naval Operations Adm. Gary Roughead said. "I also think you're beginning to also see the increase in the depth of the magazine chain. In other words, the capacity's going to change, because you essentially have a rechargeable projectile." Advantage United States, as the rise of lasers will lead to a geostrategic

division into “countries that can afford to go into directed energy and countries that can’t.”

The committee doesn’t think it’s worth it. It thinks the technology isn’t sufficiently proven — and, indeed, neither weapon will be ready until at least the next decade under optimal conditions. But the Navy’s got a lot of work to do to convince the Senate that its futuristic weapons are worth saving. And if those weapons get killed, it’s an open question whether *any* high-tech weapons priority for the military is safe from the chopping block.

*Photo: Office of Naval Research*

## U.S. Soldiers Push Network In Desert Trials

By MICHAEL HOFFMAN
Published: 28 Jun 2011 10:41

WHITE SANDS MISSILE RANGE, N.M. - U.S. Army leaders have taken the service's new network of radios, computers and smartphones out of the hands of engineers and handed them to soldiers like Capt. Phillip McCoy, who have endured deployments to Iraq and Afghanistan, to give each system a combat reality check.

Soldiers here are blunt when it comes to equipment that has made their jobs harder during the first three weeks of the Network Integration Evaluation (NIE). Caked in sand and enduring 100-degree days, they don't care how many millions have already been invested, or whose congressional district might benefit from a new Army contract. They just care if it works.

Ground Mobile Radio (GMR), a product of the canceled Future Combat Systems program, fails that test.

"GMR has been nothing more than a heavy paperweight," said McCoy, the battle captain for the battalion tactical operations center. In field tests here, he said, the radio has consistently overheated and left soldiers disconnected from the network.

"They need to go back to the drawing board on that one because I wouldn't want to take that out of here," he said.

The Spider XM7 Network Command Munition fared better, according to soldiers.

Capt. Matt Davis, a battery commander for 4th Battalion, 27th Field Artillery Regiment, said he has seen progress since he tested GMR last year, but said his soldiers must constantly run their vehicle's air conditioning at full blast even when the truck is parked to keep it from overheating.

It's this sort of feedback Gen. Peter Chiarelli, the Army's vice chief of staff, expected when he led the charge to institute the NIE. The exercise has brought what used to be a disjointed set of separate tests of the Army's different network systems under the umbrella of a semiannual exercise here.

Chiarelli's theory: Better that the radios and computer systems fail in a war game in New Mexico than when it counts in combat in Afghanistan.

"The vice took a look at this and said what a lot of people were thinking: 'This doesn't make sense, we need to change this and get these systems in the hands of soldiers before they make it to combat.' We needed that person to lead the charge," said Col. John Wendel, deputy program executive officer, integration.

GMR is just one of many network systems that service officials will evaluate. Others include the Joint Tactical Radio System (JTRS), the Mounted Soldier System, the next-generation Force XXI Battle Command Brigade and Below system, the Network Integration Kit, the JTRS Handheld Manpack Small Form Fit radio and the Spider XM7 Network Command Munition.

Early results show soldiers have been impressed by the Spider XM7. Command Post of the Future received lower marks by the soldiers interviewed for this article.

Most officials and soldiers at White Sands said it was too early to judge results, but they have received plenty of feedback. Whether the network works flawlessly isn't the objective, Wendel said. The point is to identify problems early.

"The Army isn't here to buy radios. We want to find out what works best," he said.

About 3,800 soldiers in 2nd Brigade, 1st Armored Division, will run the evaluation, as it is the first brigade taken out of the typical deployment cycle to execute this sort of exercise. Brigade Modernization Command, Army Test and Evaluation Command and PEO Integration form what is called the Triad that will oversee it.

# US Soldiers Push Network in Desert Trials

The eyes of the Army are squarely on the NIE exercise. Fifty-nine general officers will visit White Sands in the fourth week alone to see how the network and overall test model have fared.

Wendel said he could see the NIE model expanding across the Army depending on its success.

"I'd say we're pleasantly surprised at how well the first weeks have gone so far," Wendel said.

Army leaders remain bullish on fielding smartphones to combat soldiers.

The Army issued Motorola phones to soldiers in Alpha Company, 1st Battalion, 35th Armored Regiment uploaded with programs such as Soldier Eyes, which allows the user to mark areas of interest, such as the site of an improvised explosive device. When the phone is held up, a mark shows up on the screen over the imagery where the phone's camera is pointing. Soldiers also found the mapping software that walks the user onto a target useful.

"The soldiers really like the mapping aspect. The one thing they have found, though, is you don't assault an objective head on, so they need to work on that," said Capt. Scott DeWitt, company commander of Alpha 1-35.

The captain issued phones to each of his squad and platoon leaders. He said his infantry soldiers need a case that can stand up to the elements, including the dust storms they've endured at White Sands.

Most, if not all, of the soldiers in DeWitt's company have cellphones so the train-up was easy, he said. Many of the soldiers quickly navigated the phone's features and have given the engineers feedback on what applications the Army should add.

"They've grown up with this technology, so they know what they're talking about when

it comes to these phones," DeWitt said.

Army officials know they need to develop new networks and find new ways to power them.

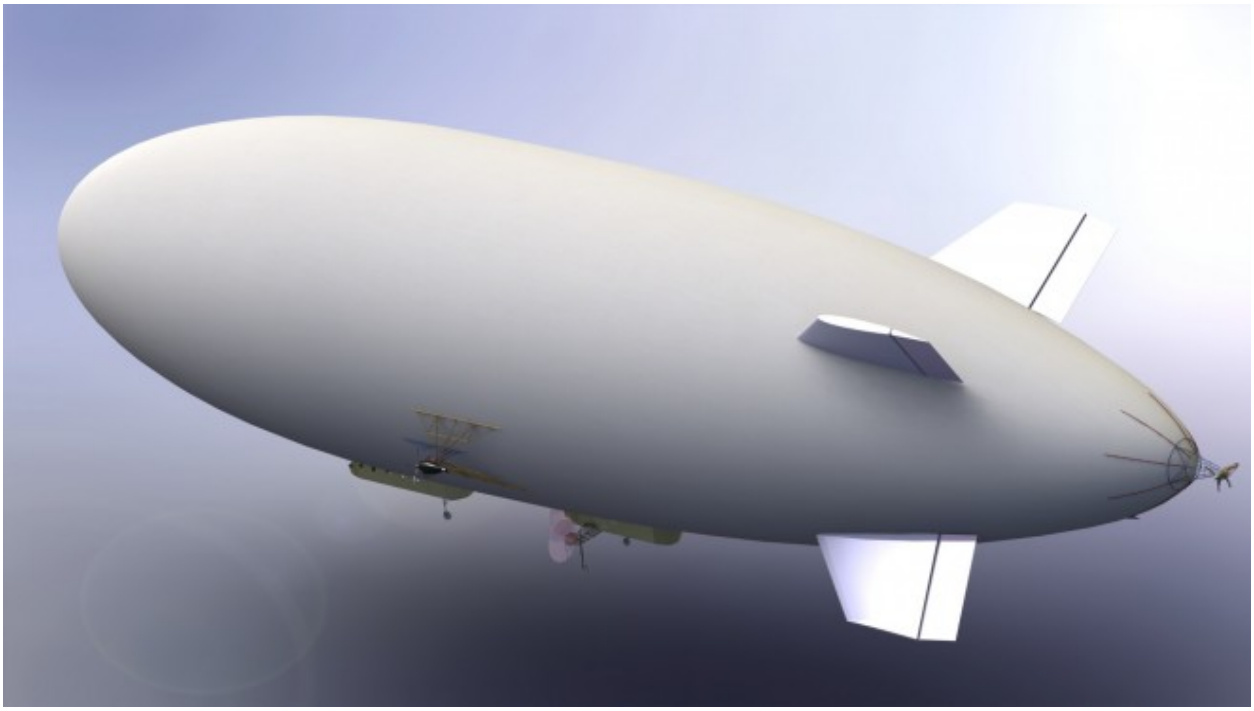
"You can't just come up with all these new systems that demand power and not provide answers to how all of this will run," said Terry Garrison, the team lead for Command Post Systems & Integration.

The Army is testing an intelligent generator built by DRASH. Each digital generator has a smart chip installed that can turn generators on and off depending on the unit's power needs.

Garrison said early estimates suggest intelligent generators could provide 13 to 20 percent fuel savings.

**Giant Spy Blimp Battle Could Decide Surveillance's Future**

- By Noah Shachtman July 6, 2011 | 7:00 am | Categories: Air Force
  **@dangerroom** · 20.6K followers



How many giant experimental spy blimps does the military need over Afghanistan, exactly?

That's one of many questions the Senate Armed Services Committee is asking after an intramilitary battle has erupted over what many expect to be the future of aerial surveillance. The Army and the Air Force each have their own football field-sized airships in the works; the Senate panel wants to know why it should pay for both — especially as the Air Force seems fickle about its model and keeps changing the spy sensors on board. Legislators are asking: What gives?

This is more than some obscure bureaucratic hair-pull. The answer to those questions — and the winners of those fights — could determine the direction of U.S. intelligence-

gathering for years to come.

Here's why. Surveillance drones like the Predator and the Reaper are starting to lose just a bit of their sheen in military circles, even though their number of "orbits," or combat air patrols, has more than quadrupled in the last five years. Giant spy blimps are the new hotness. They can stay in the air for much longer than any drone. Instead of a Predator's single camera, the blimps can carry a whole bunch of surveillance equipment, because they're so freakin' huge. Any one of those sensors could spy on an entire town at once. There's even enough space on board the airship to process all that data in the sky, easing the burden on overloaded intelligence analysts.

A sign of the spy blimp's rising stock: Retired Lt. Gen. David Deptula — who, until recently, was in charge of all Air Force intelligence, surveillance and reconnaissance (ISR) programs — is now the CEO of MAV6, a Vicksburg, Mississippi, startup building one of these next-gen airships for the military.

It's part of a project called "Blue Devil." The behemoth, 340-foot-long blimp and all of its spy gear should be ready for Air Force duty by January, Deptula promises. And if Blue Devil works as promised — staying four miles above Afghanistan for five days at a time — drones could suddenly seems like an expensive anachronism.

"It brings to bear a completely different concept for ISR: multiple sensors on one platform integrated with on-board processing and storage. It's the first time we're using a modular system on an aircraft to host a variety of sensors, and they can be rapidly changed for new or different sensors in a matter of hours," Deptula tells Danger Room. "We've got the world's largest ISR payload — and 'real estate' to host it, and nearly a supercomputer on board to process what they find."

The Pentagon is planning to spend $4.5 billion to mount 15 more drone air patrols. The costs of operating, maintaining and processing the information from the roboplanes runs about $8,000 per hour. Deptula claims Blue Devil would run $1,000 per hour, because it requires fewer people (although that's just an educated guess; the thing hasn't flown yet). "A handful of Blue Devil orbits could achieve significantly greater ISR effectiveness for a fraction of that cost and save billions," he insists. For now, the Air Force is spending $211 million on one of Deptula's blimps.

The Senate Armed Service Committee digs the idea. "There are many platforms and systems that advertise 'multisensor integration,' but almost always the different sensors … cannot view the same piece of terrain at the same time," the committee notes in its recent report on next year's Pentagon budget. "Blue Devil is different: this QRC [quick reaction capability] is designed to give ground forces a new capability to detect, locate, identify, and track targets seamlessly, building on concepts and practices pioneered by special forces to tightly integrate sensors and pursuit operations."

But the committee "is concerned about recent turmoil in program plans," according to the report. For starters, Blue Devil isn't the only ginormous airship heading for Afghanistan. The Army has one in the works, too.

It's called the Long Endurance Multi-Intelligence Vehicle, or LEMV. It's being built by Northrop Grumman, the defense contracting behemoth. It's allegedly going to start casting its "unblinking eye" by January. And the LEMV supposed to stay in the skies for *weeks*, thanks to a combination of lighter-than-air helium and the aerodynamic lift you'd ordinarily see in an airplane. Initial cost: $517 million, for three airships. But, according to InsideDefense.com, the Pentagon is already asking for another $28 million.

Which naturally has lead the Senate Armed Service to ask why we need both of these

things.

“These developments raise the question of the value of Blue Devil Block 2,” the committee report reads.

“The Army now plans to deploy the LEMV to Afghanistan in the same timeframe as Blue Devil Block 2. Moreover, the Army is now planning to rapidly equip LEMV, after it is first demonstrated, with the same sensor systems that were originally planned for Blue Devil Block 2,” the committee adds. “The sensor changes raise questions about how effective and useful it will be, while progress in the LEMV program raises the issue of whether Blue Devil Block 2 funds would be better invested in LEMV program acceleration and expansion.”

LEMV may not be able to stay in the air quite as long as advertised. A recent technical presentation (.pdf) noted that the airship might stay aloft for a mere 10 days at a stretch.

Yet the Air Force is showing some signs of ambivalence about its Blue Devil airship. Turns out, the air service has grown rather attached to its current gaggle of spy planes.

That’s ironic, since it wasn’t that long ago that Defense Secretary Bob Gates complained that getting the Air Force to field more Predator and Reaper drones was like “pulling teeth.” The upstart robo-planes were a threat to the air service’s established, man-in-the-cockpit fleet. Now, however, the upstarts have become the establishment. Drones form the bedrock of the Air Force’s surveillance effort.

“Big Safari” — that’s the code name for the Air Force office in charge of special intelligence programs — doesn’t appear to be quite ready to shift gears again. Especially not when shifting gears means putting a small company like Deptula’s in

the driver's seat.

"The Air Force transferred responsibility for Blue Devil recently to the Big Safari Program Office, which promptly proposed wholesale changes to the program — an entirely different platform, continued use of legacy [c]ameras, and different SIGINT [signals intelligence] sensors," the Senate report notes.

Most of those changes were ultimately beaten back. But there are still open issues about the future of Blue Devil — and how the airship relates to its past.

The Blue Devil program started by packing a bunch of sensors together onto a turboprop plane. That surveillance gear includes eavesdropping equipment that can pinpoint a chatty militant's location, as well as the Angel Fire "wide-area airborne surveillance system," or WAAS. It's a hive of nine separate cameras, each one shooting at a very slow rate and at a slightly different angle — allowing a whole town to be watched at once.

On the Blue Devil turboprop plane, the WAAS sensors and the eavesdropping unit can tell each other where to look or listen. According to the committee, that combo is now "making significant contributions" in southern Afghanistan, "particularly in support of prosecuting high-value targets." In other words, it's helping the military hunt down and kill militants.

But Deptula — and the Air Force — don't just want to move that gear onto the airship for the second phase of Blue Devil. There's talk of upgrading the WAAS sensor, from nine cameras to 92. Plus, the blimp has room for more and bigger antennas. And the more and bigger antennas you have, the easier it is to pinpoint locations. The blimp could be a much better eavesdropper. The Air Force and the ear-men at the National Security Agency are still wrestling over which signals intelligence package will fly on

the airship.

Even muddier is the Air Force plan for what to do if the spy blimp wows the military if and when it goes to Afghanistan; there's no follow-on effort in the budget, at the moment.

Making things murkier still is that there are *two more* giant blimp programs making their way through the military's development chain.

The Armed Services Committee is kind of fed up. It's demanding that the Pentagon appoint a single point person who can sort out which airship projects make sense, and which don't. This is *supposed* to a time of coming budget cuts, after all. The sky is pretty big. But it's not big enough for all these king-sized blimps.

*Illo: Mav6*

# Army's Antennae in the Sky

The Army’s antennae in the sky

By Philip Ewing Thursday, July 7th, 2011 4:00 pm

No satellites? No problem. Army officials say they can expand the range of their Joint Tactical Radio Systems by deputizing unmanned aerial vehicles as relay stations, according to an official story this week about the ongoing network test at White Sands, N.M. Blimps and the Army’s Shadow UAV both can carry JTRS equipment that increases the distance over which soldiers can talk to each other, keeping everyone on the battlefield connected without the need for a satellite link.

Per the Army’s story:

The Aerostat blimps being used in the [Network Integration Evaluation] are carrying a four-channel, software-programmable JTRS Ground Mobile Radio as well as two-channel JTRS Handheld Manpack Small radios. The Shadow UAS are engineered to carry single-channel JTRS Rifleman Radios.

The idea is to expand a terrestrial, JTRS-based communications network by adding aerial nodes designed to extend the ability to relay information across further distances through line-of-sight connections. The software-programmable JTRS radios, which can make use of encryption to safeguard information, are built to send IP packets of data, voice, video and images via multiple waveforms between static command centers, vehicles on-the-move and even dismounted individual soldiers on patrol.

“The aerial layer allows RF [radio frequencies] to travel further and more freely. It gets you line-of-sight connections to additional nodes on the network,” said Jerry Tyree, deputy for material at Brigade Modernization Command. “We’re getting ranges greater than 60 kilometers with the aerial layer.”

Part of the rationale for JTRS technology is to afford battlefield communications in an austere environment where satellite technology might not always be available.

Commanders hope that expanding the breadth of these networks will let everyone in the battle space — on foot, in vehicles, in the air or back at the FOB — stay on the same page.

Airships for the 21st Century

Long-duration, heavy-lift designs breathe new life into the world's oldest aircraft technology

By RON HOCHSTETLER / OCTOBER 2010

Illustration: Science Applications International Corp.

**Residents of Caribou, Maine, who happened** to glance up at the skies over the former Loring Air Force Base recently got a glimpse of the future—although they might have thought they were looking at something out of the past. Engineers from my company, Science Applications International Corp. (SAIC), in McLean, Va., have been conducting test flights of a new type of lighter-than-air vehicle.

In appearance, the Skybus 80K bears the same oblong shape as the Goodyear Blimp, and it's based on the same flight principles that have governed airships since the 1800s. But this airship, one of a number of commercial and military vehicles now under development, represents a distinct break from tradition. Unlike their dirigible cousins of past centuries, these new vehicles are being designed to lift heavy payloads, remain aloft for weeks or even months at a time, and fly without pilots—all

while expending far less energy than a conventional airplane or unmanned aerial vehicle. The Predator UAV, for instance, can carry a payload of 340 kilograms on a typical mission of up to 40 hours. SAIC's Skybus 1500E pilot-optional airship is being designed to carry a payload three times that size and stay aloft for up to 21 days.

The renewed investment in airships comes at a time when the energy footprint of all modes of transportation is being scrutinized. Some aviation visionaries now argue that we can't continue using exclusively petroleum-based fuels to power our aircraft. Such concerns have prompted new research into jet biofuels and energy-efficient jet engines. We've also begun to understand that not every flight has to be made at eight-tenths the speed of sound. For certain tasks, airplanes just can't compete with airships. Modern airship designers are targeting two pressing needs: intelligence, surveillance, and reconnaissance missions and the transporting of multiton payloads to locations unreachable by conventional transport. For example, airships are ideal for continuously monitoring sites where improvised explosive devices or rocket launchers may be deployed. They also excel at scanning for distant airborne threats. That's why, in June, the U.S. Army awarded a US $517 million contract to Northrop Grumman and British firm Hybrid Air Vehicles to build three airships, each as long as a football field, to monitor trouble spots in Afghanistan. Cargo airships, meanwhile, are especially attractive for places that have poor roads and for remote regions that have no roads at all. At a transportation conference I recently attended in Canada's Northwest Territories, mining company executives and community leaders expressed strong support for using airships to shuttle equipment and supplies to distant mining outposts and villages. Such needs are driving the reinvention of the airship.

(A full transcript of this video is available on the video page.)

**An airship flies primarily by Archimedes's** principle, which describes the buoyancy of a body submerged in a denser fluid. That is, an airship operates more like a submarine than an airplane or a helicopter. Those aircraft have to generate 100 percent of their lift from the flow of air over their wings or rotor blades. An airship, however, employs a lighter-than-air nonflammable gas such as helium to give it buoyancy. When the lifting gas displaces a volume of air that weighs more than the

entire airship (including fuel and payload), the airship floats. That resultant lift is what's known as the airship's static buoyancy. For instance, to lift 1 kilogram at sea level, the airship needs approximately 1 cubic meter of helium gas. Airships weigh considerably more than that, of course; the Skybus that recently flew in Maine tipped the scales at 1600 kg unfilled.

The lifting gas is contained within the airship's outer skin, a large fabric bag or envelope that is aerodynamic, lightweight, and rugged. Inside the envelope are one or more smaller bags, called ballonets, which hold ordinary air. On the ground, electric fans pump air into the ballonets until the pressure of the helium surrounding the ballonets exceeds atmospheric pressure by a very slight margin of about 480 pascals. The ballonets occupy between 25 and 50 percent of the airship's total gas volume. Bleeding off a measured amount of air through valves in the ballonets provides room inside the envelope for the helium to expand as the ship rises.

As the airship ascends, the decreasing atmospheric pressure causes the helium inside the airship to expand steadily. Once all the air in the ballonets is gone, the airship cannot ascend higher without either bursting or venting its helium. This point is known as the airship's pressure altitude. To descend, the airship uses its electric fans to blow air back into the ballonets. This gas-management system must constantly keep the helium at a pressure that's slightly higher than the surrounding atmosphere, to preserve the aerodynamic shape of the envelope.

If ascending and descending were all an airship did, this combination of gases and ballonets would be sufficient. But an airship also needs a certain amount of power and propulsion, to run the onboard navigation and communications systems and any electronics in the payload, and to maneuver to different locations. Most current airships use traditional gasoline engines, but increasingly designers are looking at alternative power and propulsion systems. One idea is a regenerative system incorporating photovoltaics and fuel cells, in which hydrogen fuel cells produce water vapor. The solar power could be used to separate the water back into its component gases; the hydrogen would then be fed back into the fuel cells.

Almost all airships flying today are of a nonrigid design, which means the ship's shape

comes only from the pressure of the gases inside. By contrast, the giant airships of the 1930s, the *Hindenburg* being the most iconic example, had rigid internal skeletons made of aluminum or wood. Inside this cage were a dozen or more gas-filled lifting bags. Those days also saw the development of semirigid designs, which typically had a stout aluminum keel running lengthwise from the nose to the tail, providing a convenient mounting point for the individual gas cells and distributing the lift of each cell evenly. The only semirigid airships flying today are the Zeppelin NT series, which began operations in the late 1990s and are used primarily for sightseeing and advertising.

Illustration: Boeing
**UP THERE:** The SkyHook airship, a joint project of Boeing and the Canadian company SkyHook International, is a rotary-airship hybrid that will haul oil-drilling equipment in northern Canada.

Although nonrigid airships aren't weighed down by an internal framework, they still have to support the gases, fabric, and other components, as well as any payload. Obviously, the greater the airship's weight, the larger the volume of lifting gas needed and the bigger the envelope size. As the size increases, so does the vehicle's surface area and consequently the amount of aerodynamic drag during flight. These and other factors dictate the amount of power required to propel the airship through the sky.

**Although people pilot most of today's** airships, the newer designs are increasingly pilot optional, meaning that a crew can fly them during tests or initial deployments and then quickly switch them to remote operation. Several fully remotely operated airships are also in development. One of their chief uses right now is for battlefield surveillance. These airships carry various imagers and detectors to altitudes of 1500 to 5500 meters on missions lasting 24 hours or more. Guardian Flight Systems, based in North Carolina, developed the pilot-optional Polar 400 for the U.S. Department of Defense. In the fully pilotless category is SAIC's Skybus 80K airship, which so far has conducted more than 62 hours of flight tests in Maine. To date, the Skybus 80K is the only unmanned airship to hold an experimental designation from the U.S. Federal Aviation Administration. It has a gas volume of 2300 m3 (80 000 cubic feet) and is designed to carry a 230-kg surveillance payload as high as 3000 meters for up to 24 hours.

More ambitious is the U.S. Army's Long Endurance Multi-Intelligence Vehicle. The LEMV will carry a 1100-kg payload up to 6000 meters for as long as 21 days without refueling. Its first deployment is to be in Afghanistan in late 2011 or early 2012. A number of defense companies considered vying for the LEMV contract. But two months ago, the five-year contract—one of the largest airship contracts to be awarded since World War II—went to Northrop Grumman and Hybrid Air Vehicles.

To operate in the thin atmosphere at such high altitudes for extended periods of time, an airship needs to be light (at least compared with lower-flying counterparts) and have an efficient propulsion system that can function with little or no oxygen. Also

essential is a design that minimizes aerodynamic drag, which is why high-altitude airships almost always have the familiar ellipsoidal shape. Among the power sources being considered for high-altitude airships are electric motors coupled with lithium-ion batteries, hydrogen fuel cells, and flexible-film photovoltaics, which would blanket the upper parts of the airship's huge surface. Any of these options would need to weigh less and be more efficient than standard engines.

To fly even higher and longer with heavier sensor payloads is the ultimate goal of military leaders who see the modern airship as an unblinking, ever-present eye in the sky. Under the Defense Department's $149 million High Altitude Airship program, Lockheed's Maritime Systems & Sensors Division in Akron, Ohio, is now exploring ways to build an airship capable of carrying a 230-kg sensor package into the stratosphere, as much as 18 kilometers up, where it would remain for a month at a time. At that altitude, one airship would be able to monitor a patch of ground 1200 km across. Just 11 of them could provide radar coverage of the coastal and southern borders of the continental United States, according to the North American Aerospace Defense Command.
If that sounds ambitious, consider the proposed high-altitude airship known as the Integrated Sensor Is Structure, or ISIS. Under this $400 million program jointly funded by the Defense Advanced Research Projects Agency and the U.S. Air Force, Lockheed's Skunk Works is building an unmanned stratospheric airship powered by solar cells and fuel cells that would be capable of operating at 21 kilometers' altitude for up to 10 years at a time. A one-third-scale prototype, itself longer than a football field, is scheduled to fly in 2013.

What makes ISIS unique is the integration of its mission sensors—a UHF radar for monitoring vehicles and soldiers on the ground and an X-band radar for tracking cruise missiles up to 600 km away—into the body of the airship. According to Raytheon, which is building the radars, the radar antennas form a cylinder in the center of the airship. By integrating the sensor system into the structural supports, the design reduces the airship's overall weight and adds structural stiffness. Even so, the demands of a 10-year high-altitude mission mean that the full-scale ISIS will need to be made of extremely durable, yet lightweight materials—materials that may not yet exist. In addition, its power system will need advanced photovoltaics and fuel cells

capable of generating enough power to operate the radars, navigation system, communications gear, and the electric motors that will turn the airship's giant propellers. A lot of extreme engineering is going into today's airship designs.

**While the upcoming stratospheric** surveillance airships will carry relatively small payloads, some airships now in development will lift a great deal more—payloads of hundreds of tons, albeit at lower altitudes. That presents an entirely different set of challenges.

An airship designed to carry 50 metric tons of cargo would be hundreds of meters long and weigh tens of tons lying empty of helium on the factory floor. The sheer size would make its assembly a daunting task. These new vehicles would likely be built in smaller subsections that would later be joined together in immense hangars.

A more critical issue is how to compensate for the sudden increase in the airship's static lift that occurs when a heavy payload is unloaded. The most straightforward remedy is to add onto the airship an amount of weight equal to the payload as the payload is removed.

Some heavy-lift designers are also developing hybrid vehicles. These incorporate the static lift of helium along with some form of dynamic lift, such as helicopter-style rotors or airplane-like wings. In most of these designs, the helium is sufficient to lift the vehicle's weight, while the dynamic lift is devoted to the payload's weight. This produces an aircraft that is slightly heavier than air and so is much less buoyant during cargo unloading.

Illustration: Northrop Grumman
**EYE IN THE SKY:** The U.S. Army's pilot-optional Long Endurance Multi-Intelligence Vehicle will conduct surveillance in Afghanistan. Northrop Grumman and the British firm Hybrid Air Vehicles recently won the $517 million contract to build the hybrid airship.

Lockheed's Skunk Works first test-flew its P-791 proof-of-concept hybrid airship in 2006. The aircraft has two propulsion motors on the exterior of its envelope and two attached to its tail. This generates about 20 percent of the dynamic lift when the vehicle is flying forward. Other hybrid airships under development include Hybrid Air Vehicles' SkyCat, which will be the basis for the U.S. Army's LEMV; the Worldwide Aeros Corp.'s Aeroscraft, which was recently submitted to the FAA for design certification; and the proof-of-concept Dynalifter, being readied for test flight by Ohio Airships.

While these hybrids hold promise, they also have some inherent technical challenges. For one, the additional dynamic lift increases aerodynamic drag. To help with

generating dynamic lift, they also typically have a flatter profile than conventional airships, but this shape gives them a higher ratio of envelope fabric to gas volume, increasing the airship's empty weight. Higher weight and drag, of course, mean more propulsive power and more fuel, both of which make the ship even heavier. And some hybrids employ multiple lobes in their design, which can create problems as the gases inside heat up from the sun's rays. Helium conducts heat six times as efficiently as air, so a multi-lobed hybrid may tend to list toward the side that's not exposed to the sun.

Perhaps the biggest issue, though, is the hybrid's potential to pitch nose up or down and to roll from side to side. A conventional, single-hulled airship avoids this problem because the majority of its gas volume is positioned well above its center of gravity, imparting what's known as pendulum stability. The higher up the center of lift is, the more stable the airship is; conversely, the closer the center of lift is to the center of gravity, the greater the tendency of pitching from wind gusts.

To get around these problems, Boeing and the Canadian company SkyHook International are collaborating on a different approach: a rotary-airship hybrid. It combines a conventional ellipsoidal envelope with four powerful helicopter rotor units, which are installed below the helium envelope. The helium is sufficient to support the weight of the vehicle itself, leaving the full power of the rotors to lift a 36-metric-ton payload. One of the first applications of the SkyHook is moving equipment and supplies for oil-drilling operations in northern Canada.

To spur further progress in heavy-lift designs, I and several other airship enthusiasts are setting up an international contest to promote the development of airships as a green, low-carbon form of cargo transport for commercial operations. The Zero Emissions Transport Airship Prize, or Z-Prize, similar to the more familiar X-Prize, will offer a large cash award for the successful development and flight test of a heavy-lift airship that meets the competition's criteria. We hope to entice airship developers to focus their efforts on designing cost-effective cargo airships that will have their greatest applications in developing regions—places where moving freight by conventional transport is difficult and hugely expensive or subject to disruption by criminals or terrorists. And by emphasizing airship designs with low carbon emissions, we hope also to encourage the creation of the first environmentally sustainable air-transport

system.

It's an exciting time to be an airship engineer. These vehicles represent both the oldest and now the latest forms of aircraft. They're also an aviation technology that has yet to be fully exploited. While some naysayers may think the time of these leviathans is long past, in fact their day is just dawning.

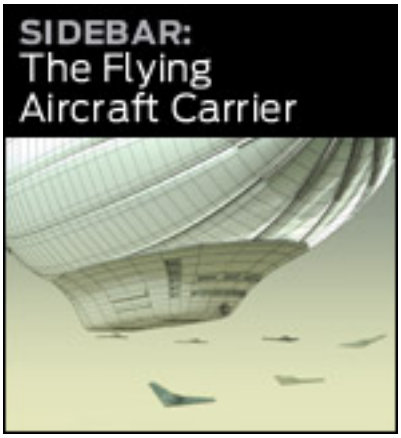
*This article originally appeared in print as "Airships Ahoy".*

**About the Author**

Ron Hochstetler is director of lighter-than-air programs for Science Applications International Corp., in McLean, Va. For more about the author, see the Back Story, "Up in the Air."

**To Probe Further**

For more about modern airships, see the accompanying video, "Airship Renaissance."




**The Flying Aircraft Carrier**

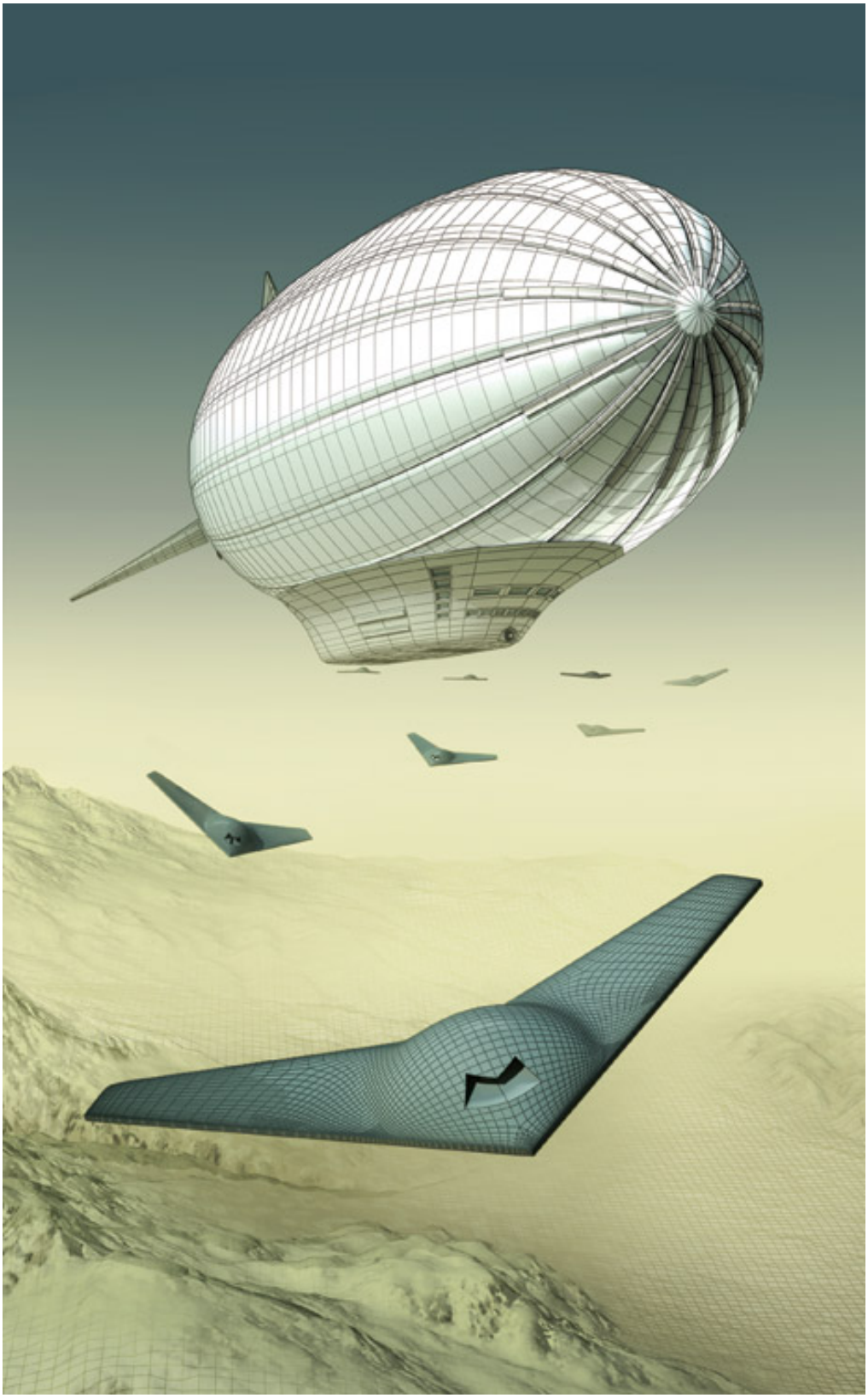


Illustration: Emily Cooper

Back in the 1930s, the USS Akron and USS Macon, two U.S. Navy airships, supported a small squadron of scout biplanes from internal aircraft hangars in their huge bellies. A modern version of this concept would be an airship designed to carry dozens of small, low-cost, unmanned aerial vehicles (UAVs), each equipped with miniaturized sensors, antisubmarine warfare systems, or even lightweight precision weapons. This pilot-optional airship could serve as a sky base from which the UAVs would launch, refuel, and relaunch. The airship itself could also be designed to be refueled in flight, meaning that the entire system could serve as an almost permanent airborne platform. To minimize its vulnerability to attack, the airship would be positioned away from any areas of conflict into which the UAVs would be deployed. Equipped with its own lightweight self-defense systems, this flying aircraft carrier could be a game-changing military system

**The Sailing Airship**

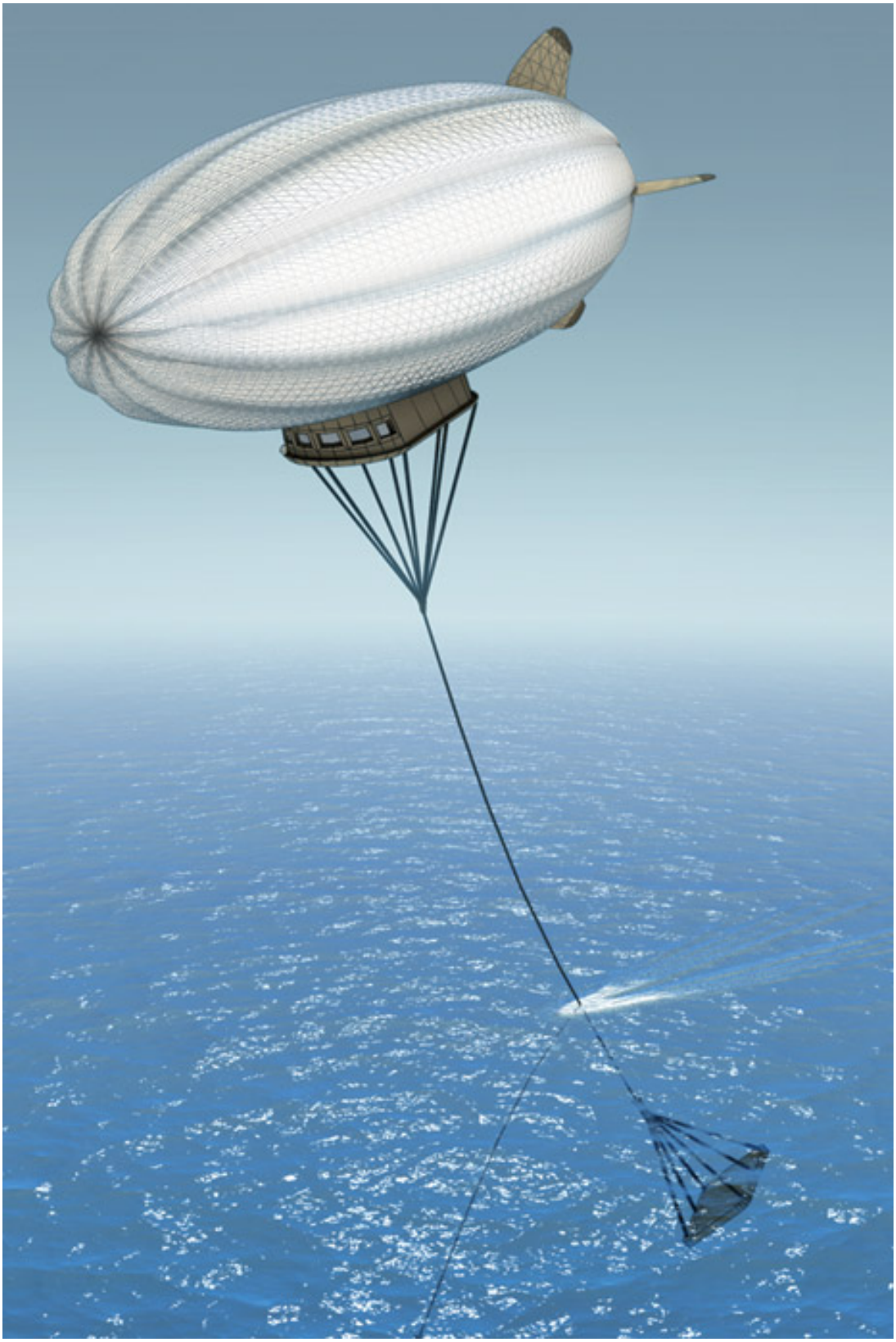
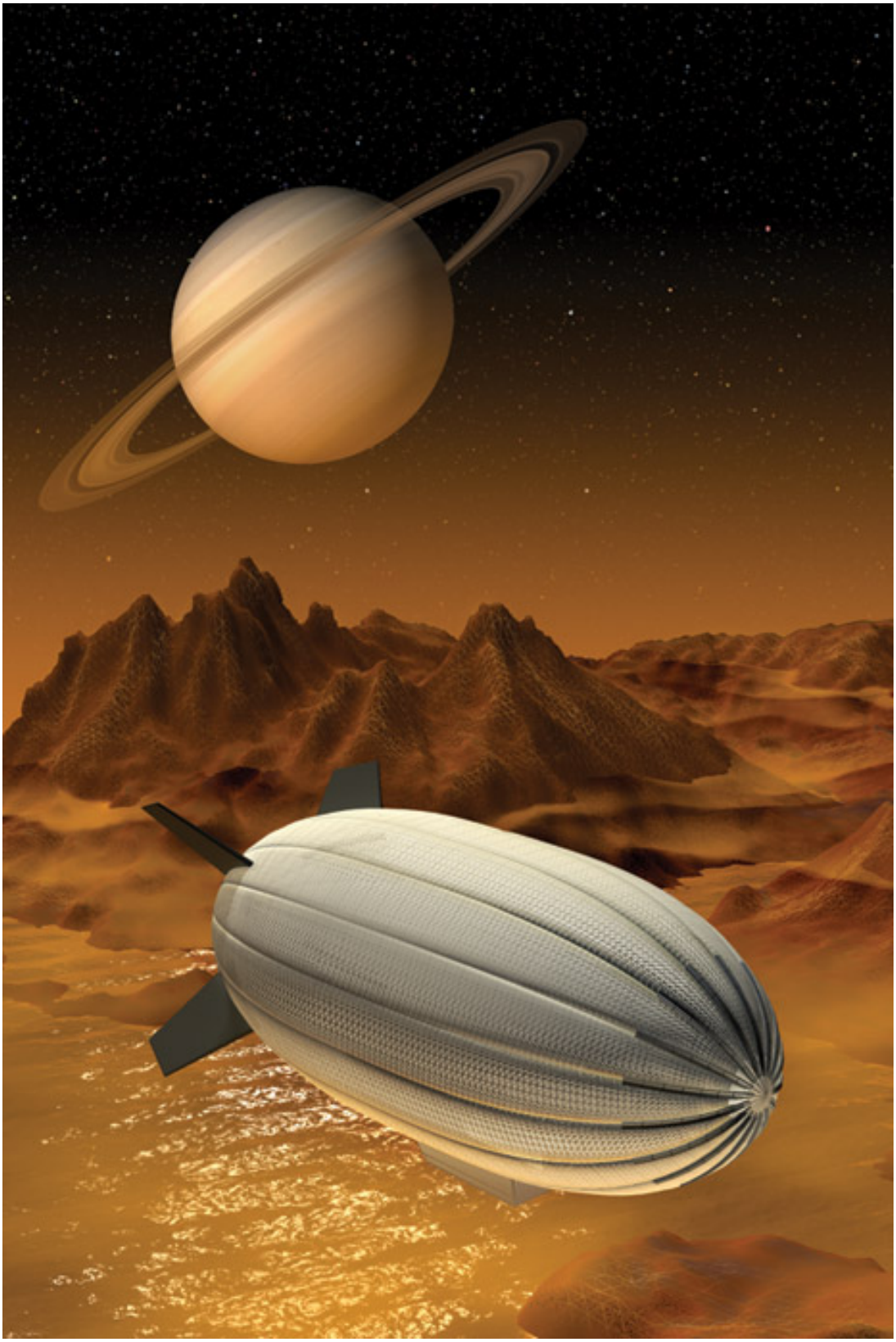


Illustration: Emily Cooper

In 1940 the noted American airship engineer Charles P. Burgess speculated that it might be possible to sail an airship at sea. He proposed lowering from an airship by cables a hydrodynamic body that would serve as an underwater wing, translating the force of the wind blowing on the airship into controllable motion through the water. The airship's great surface area, he suggested, would capture enough wind to allow it to be used for dedicated transoceanic airships. To date, nobody has realized Burgess's vision, but it would surely represent the greenest of air-transportation systems.

**Airships in Space**



# Airships for the 21st Century

Illustration: Emily Cooper

Earth isn't the only place where airships could find a home. A number of off-world destinations have enough of an atmosphere to support airships, including Mars, Venus, and Saturn's largest moon, Titan. Compared with robotic rovers, airships would be able to survey far more ground. And they don't require much power, which is always at a premium on planetary missions. So far, the only successful extraterrestrial deployment was the Soviet Union's 1984 Vega mission to Venus, which sent two balloons to float 54 kilometers above the planet's surface for nearly two days.

More recently, NASA has funded a number of balloon and airship projects for solar system exploration. Researchers at the Jet Propulsion Laboratory in Pasadena, Calif., have developed several lighter-than-air designs for use on a possible follow-up mission to Titan and Venus. They've also conducted extensive flight tests over the Mojave Desert with an 11-meter-long autonomous airship. There's even talk of sending entire fleets of rovers and airships to scout out new planetary frontiers.

# UCAS Demonstrator Clears Key Milestone in Sea-Based Qualification Testing

**UCAS Demonstrator Clears Key Milestone In Sea-Based Qualification Testing**
*(DEFENSE DAILY 06 JUL 11)* ... Carlo Munoz

The Navy and industry team developing the Unmanned Combat Air System Demonstrator (UCAS-D) for the sea service cleared a critical milestone this month, proving the system's ship-based command and control software could perform in a maritime environment.

The UCAS-D software was used to control multiple launches and recoveries with a "manned surrogate aircraft" aboard the USS Dwight D. Eisenhower (CVN-79) late last week. While manned, the surrogate aircraft was outfitted with the avionics and control systems designed for the actual UCAS-D aircraft, built by prime contractor Northrop Grumman [NOC], according to a company statement.

"Using a manned surrogate platform to test the unmanned systems avionics and software gives us an extra layer of safety as we test the [UCAS-D] software to ensure that it responds correctly and safely to different flight conditions," Glenn Colby, aviation and ship integration lead for Navy Air Systems Command, said in the statement.

The successful control and navigation capabilities demonstrated between the on board C2 software and the UCAS-D navigation and avionics systems in flight in a maritime environment puts the program well on track to hit a first unmanned, carrier-based flight test goal of 2013, a senior Navy program official said.

"This manned surrogate test event is a significant and critical step toward landing the [UCAS-D] on the carrier deck in 2013," Navy Program Manager Capt. Jaime Engdahl said in the same statement. "It represents the first end-to-end test of the hardware and software systems that will eventually allow unmanned systems to integrate safely and successfully with all aspects of carrier operations."

Results from the surrogate testing will be used to continue to refine the mission management, navigation, guidance and control software that the [UCAS-D] will use to perform its first carrier landings in 2013, the statement adds.

Northrop Grumman officials completed the avionics software development for the UCAS-D late last month, company officials told Defense Daily at the time. The completed software tested during last week's sea trials will be the precursor to the avionics setup that will actually control the air vehicles during unmanned carrier trials at sea.

That final avionics software is currently undergoing testing and should be complete by the end of this year, company officials added.

The biggest challenge facing program officials during last week's shipboard testing was ensuring the established checks and communications between the aircraft and ship--usually conducted by the pilot--maintain the same level of rigor under the newly automated process for the UCAS-D.

"Today's carrier environment relies on human operators to monitor and ensure safe flight operations," Colby added. "As we begin to integrate unmanned systems into this very restrictive manned environment, we have to ensure that the software controlling these new systems can

recognize and respond correctly to every type of contingency."

While the flight tests represent a major milestone for the UCAS-D program, the results will also have a large impact on the Navy's follow-on program, the Unmanned Carrier-Launched Surveillance and Strike (UCLASS) aircraft.

The UCAS-D, as envisioned by Navy planners, will be an unmanned, carrier-based intelligence, surveillance and reconnaissance aircraft with the ability to carry out precision strike operations. Navy officials hope to have either a UCLASS or UCAS-type system deployed with the fleet's carrier groups by 2018.

Along with Northrop Grumman, the Navy has issued a total of just over $1 million in research and development funds via four separate contracts to Boeing [BA], General Atomics Aeronautical Systems, and Lockheed Martin [LMT] in late June, as part of the sea service's effort to get its unmanned, carrier-based aircraft concept off the ground.

Each company was awarded roughly $500,000 apiece to provide a conceptual demonstration of the Unmanned Carrier-Launched Surveillance and Strike (UCLASS) aircraft, according to a Navy release posted on the Federal Business Opportunities website.

"Proposals must have a strong emphasis on an open, adaptive architecture and disciplined systems engineering," the announcement notes. "The program anticipates leveraging existing, deployed [Defense Department] systems to launch, recover, and control the air vehicle, transfer data in support of time critical strike operations, and conduct [persistent] ISR operations."

The first of the two UCAS-D aircraft, "Air Vehicle One" is scheduled to arrive at Naval Air Station Patuxent River, Md., this fall to prepare for land-based carrier flight trials. Air Vehicle Two will follow shortly thereafter, once initial flight tests at Edwards AFB, Calif., are complete.

**Aegis ACB-12 Passes Live-Aircraft Tests**

*(AVIATION WEEK 05 JUL 11)* ... Michael Fabey

Lockheed Martin took a major step toward the development and delivery of its ACB-12 Aegis SPY-1 radar system with a recent test of its multi-mission signal processor (MMSP) against live aircraft, the company says.

The radar—which combines air and ballistic missile defense (BMD)—successfully identified, tracked and conducted simulated engagements against live aircraft in a "stressing electronic-attack environment," according to the company.

Essentially, Lockheed took Navy-supplied commercial Learjets that were "instrumented up with sophisticated jamming equipment" and flown at the Aegis radar system to test how well it would operate under a simulated attack, says Jim Judd, Lockheed technical director for ACB-12, also called Baseline 9.

The tests also yielded a "wealth of data" that will further help Lockheed meet its November 2012 delivery date to turn the upgraded Aegis system over to the Navy, Judd says. The certification should take another year.

"We're still a long way from certification," says Brad Hicks, Lockheed vice president of naval radars. But, he says, "The success of this test confirms the system is on track for deployment."

While Aegis systems have been an air defense mainstay for decades, the ACB-12 upgrades enable the ship to more effectively perform BMD missions, which have taken on a much higher priority for the Navy and the administration.

The BMD-enhanced Aegis systems prompted the Navy to restart the DDG-51 Arleigh Burke destroyer line to equip the vessels with ACB-12 and its MMSP. As part of the Aegis Modernization Program, MMSP is scheduled for installation on guided missile destroyers currently equipped with the Aegis Weapon System starting in 2012.

The recent test put the air-defense components through the wringer with the ACB-12 MMSP configuration. "This was a complicated and demanding scenario," Hicks says.

The next big test for ACB-12, scheduled for November, will run the system through similar air-defense scenarios while also simulating BMD tasks—a major event for the enhanced Aegis package.

Judd says the ACB-12 schedule is still challenging, but the recent test results show Lockheed now has a stable system and platform. "We can now move forward with incremental development," he says.

## DoD CIO duties not going to Cyber Command

July 5, 2011 — 7:50pm ET | By David Perera

Duties of the Defense Department chief information officer won't be transferred to Cyber Command, says an undated DOD memo posted online July 5. The memo is signed by Robert Gates, who left the secretary of defense position July 1.
According to the memo, Gates in December 2010 "tentatively agreed to a conceptual approach" under which significant responsibility for the operation of DoD networks would have transferred away from the DoD CIO and Defense Information Systems Agency to Cyber Command.

But, "significant policy, operational and practical concerns" prevent that course, meaning that the DoD should return to its original plan to pare down responsibilities of the DoD CIO. The DoD CIO is also the assistant secretary of defense for networks and information integration; the current CIO/ASD(NII) is Teri Takai.

Gates' memo directs that acquisition oversight of major automated information systems and responsibility for netcenricity and command and control systems be transferred by Sept. 30 to the undersecretary of acquisition, technology and logistics. The current USD(AT&L), more commonly known as the "acquisition czar" (or some close variation), is Ashton Carter.

The memo also calls for a clearer delineation of responsibilities between the CIO, DISA and Cyber Command.

SD_Directive_Memo_on_NII_Disestablishment.pdf

# Army Network Exercise Will Shake Up Status Quo, Says Vice Chief Gen. Chiarelli

6/29/2011

## Army Network Exercise Will Shake Up Status Quo, Says Vice Chief Gen. Chiarelli

Army Vice of Staff Gen. Peter W. Chiarelli is briefed by soldiers of Charlie Troop, 1st Squadron, 1st Cavalry Regiment, of the 2nd Brigade Combat Team, 1st Armored Division, during a Network Integration Exercise at White Sands Missile Range, N.M.

WHITE SANDS MISSILE RANGE, N.M. — An unprecedented six-week field exercise here, with 3,800 soldiers of the 2nd Brigade Combat Team, 1st Armored Division, is expected to lead to sweeping changes in the way the Army tests, uses and buys new technology.

One of the Army's most ardent proponents of reforming the service's procurement system, Army Vice Chief of Staff Gen. Peter W. Chiarelli, predicts that the exercise, known as "network integration evaluation," will become a paragon for a new way of doing business.

The NIE has "exceeded my expectations," Chiarelli told National Defense June 28 during a tour of operations of Alpha Company, 1st Battalion, 35th Armored Regiment, at a combat outpost in White Sands designed to replicate combat conditions.

"I think this is going to change the acquisition process," said Chiarelli. "It has

to." One of the NIE priorities is to figure out what pieces of hardware and software will be needed to create a wireless network that can support the communications and data-sharing needs of an entire brigade -- from high headquarters down to platoons, squads and dismounted soldiers.

The Army so far has been unable to put together a cohesive network because each component is designed, developed and tested in isolation. A network, by definition, doesn't work that way. "Imagine if you asked me to show you a tank, and instead I gave you an engine, a turret and a hull," Chiarelli said. That is how the Army has been managing the acquisition of a network. Program offices deliver "great niche capabilities" that don't necessarily work together. That has to change, he said. The service's rigid procurement process for years has slowed down the pace of technological innovation.

The NIE, scheduled to end in mid-July, is the first of four semi-annual events that will influence what equipment the Army will buy for combat brigades beginning in 2013. At play are billions of dollars worth of future acquisitions of wireless communications systems, tactical radios and software.

The NIE, for the first time, allows soldiers -- the "users" of the technology -- to tell the brass straight up what works and what doesn't. Under the traditional Army procurement system, a piece of equipment goes through years of development and testing before soldiers get an opportunity to put it to use.

The NIE model is "very exciting," said Army Chief Information Officer Lt. Gen. Susan Lawrence, because it makes is easier for senior officials to hear directly from soldiers and thus make better informed decisions about how to invest in new technology. It would normally take months and years to "find out what we larned here in five minutes" talking to soldiers, Lawrence said during the Alpha Company visit.

Chiarelli said he traditional focus on individual systems such as specific radio makes and models, as opposed to emphasizing the performance of the network as a whole, has been counterproductive.

A conversation with soldiers of Charlie Troop, 1st Squadron, 1st Cavalry Regiment, for instance, revealed that the Army's prototype tactical radios have shown disappointing performance. The backpack-size variant of the Joint Tactical Radio System, soldiers told Chiarelli, is too heavy to be used by

dismounted soldiers, overheats and doesn't properly run the software. That feedback is valuable, said Chiarelli, but just because some systems are showing "warts" doesn't mean the overall network effort is doomed. "What I'm seeing ... is that there's a lot of work to be done. But the only way to do it is to get everyone on the ground and see the integration issues," he said. In the case of JTRS, the software is working but the radio boxes have problems. That is a relatively easy fix, he said. "The whole JTRS business model is that we want to build the waveforms and let anyone build the box that carries the waveform." Waveforms are the software applications that define the functions of a radio network.

Over the next two NIE events, one in the fall and one next spring, there will be measurable improvements, said Chiarelli. "What's critical is that we are forcing the program managers to get together and get out of their silos and see what each other are doing, and their disconnects."

Since becoming vice chief nearly four years ago, Chiarelli has been both a point-blank critic of the Army's procurement system and also a champion of the network project. With his tenure about to end later this year and Chiarelli headed for retirement, there is growing anxiety within many program offices involved with the NIE about who, if anyone, will continue to carry the torch.

Army Vice of Staff Gen. Peter W. Chiarelli is briefed by soldiers of Alpha Company, 1st Battalion, 35th Armored Regiment, during a Network Integration Exercise at White Sands Missile Range, N.M.

Chiarelli said he is not worried. “All these guys are going to be the champions for this,” he said as he pointed at several officers who have leading roles in the network integration effort.

Tough programs that are as technologically and politically demanding as the Army’s network, however, may require a high-level strongman to keep things moving. “Whoever follows me will do the same thing,” Chiarelli said. There is enough momentum in favor of technological innovation in the Army, as soldiers rapidly adapt new technology such as smartphones and tablet computers, into day-to-day operations, Chiarelli said. “The network is going to happen.”

## DoD Wants To Shift $920M for Intel Efforts

By MARCUS WEISGERBER
Published: 7 Jul 2011 17:47

The Pentagon has asked the U.S. Congress for the OK to shift more than $920 million for numerous intelligence efforts, including many military drone programs, according to Defense Department budget documents.

The funding transfer request comes in addition to the more than $5 billion in transfers DoD has asked Congress to approve in its annual omnibus reprogramming action. Both documents were signed June 30 by Pentagon Comptroller Robert Hale.

**RELATED TOPICS**

**Americas**

The 26-page request focuses on intelligence, surveillance and reconnaissance (ISR) programs, which are mostly used by special operations forces (SOF). The vast majority of initiatives listed in the document concern unmanned aircraft programs, including the Army's Extended Range Multi Purpose (ERMP) drone and Air Force RQ-4 Global Hawk.

The four primary defense oversight committees in Congress must sign off on the shifting of funds.

The Pentagon wants to move $6 million to procure and install a Fire Scout ground control system on a ship that will deploy in support of special operations forces. U.S. Special Operations Command wants to use MQ-8B Fire Scouts -small unmanned helicopters - to support deployments, according to the document.

In addition, DoD wants to shift $32.6 million to support procurement of radar units for nine Fire Scouts. The systems will give the MQ-8B a wide area surface search capability.

Another $1 million would be used to "develop and integrate an upgrade" Fire Scout

and its control system.

"This upgrade extends the Fire Scout's combat radius, increases its payload, and improves on-station endurance to meet the urgent SOF maritime ISR requirements outlined," the document states.

The reprogramming also seeks a $28 million transfer for 60 Scan Eagle drones.

DoD wants to shift $89.3 million to install the Battlefield Airborne Communications Node (BACN) - a system that allows different types of radios and data links to communicate with each other - on two additional RQ-4 Global Hawks.

The Air Force currently flies the BACN system on three BD-700 Global Express jets and two Global Hawks.

Another $16.2 million is sought to beef up the ERMP drone with "additional capability" for classified programs. A separate $2.8 million is wanted for classified intelligence processing initiatives.

Funds are desired to complete development of a "Wide Area Focal Array Camera" sensor for the Marine Corps RQ-7 unmanned system.

The Air Force is also seeking a $44.9 million transfer for MC-12 Liberty aircraft-related upgrades, including full-motion video modems, cockpit upgrades, data links, intelligence processing equipment and a remote-control cytological operator position.

## Global Tech Leaders Promote Open Internet

**Leaders from 34 countries, including notable technology pioneers, have released principles aimed at maintaining the Internet as a forum for open communication and expression.**

By **Elizabeth Montalbano** InformationWeek
July 05, 2011 02:48 PM

Global government and business IT leaders from 34 countries have put their heads together to come up with a set of policies to maintain the Internet as a forum for open communication and expression.
The policies are similar to ones the Obama administration developed in May to steer the country's own cyberspace-related activities so as to foster a more open, interoperable, secure, and reliable cyberspace through global cooperation. They also are in line with the administration's overall goal to promote government transparency and accountability through the use of the Internet.

A group of public- and private-sector IT leaders--including Internet pioneers Tim Berners-Lee and Vint Cerf--convened last month and developed 14 key policies aimed at ensuring the Internet can continue to foster technological and economic innovation while "concomitantly meeting certain public policy objectives, including the protection of privacy, security, children online, and intellectual property," according to a communique, which is available online.

The document was developed at a meeting of the Organisation for Economic Co-operation and Development (OECD), a global organization to promote policies aimed at improving the economic and social well-being of people around the world, according to its website.

**Data centers represent a massive investment of fiscal and human capital.**

In a blog post, White House Deputy Chief Technology Officer for Internet Policy Danny Weitzner and Karen Kornbluh, U.S. ambassador to the Organization for Economic Cooperation and Development, cited recent comments by President Obama to demonstrate the administration's commitment to keeping the Internet open and free for

everyone to use.

"As the president told a group of students in China, 'I can tell you that in the United States, the fact that we have free Internet--or unrestricted Internet access--is a source of strength, and I think should be encouraged ... the more freely information flows, the stronger the society becomes,'" according to the post.

The officials decried policy such as that taken by the government of Iran last month to disconnect Iranian Internet services from the rest of the world, and said the new policies are aimed at preventing such activity from happening.

"There are calls for greater governmental and inter-governmental, top-down, one-size-fits-all control over the Internet," they said in the blog. "If these trends continue, they risk balkanizing the Internet--with high costs in both economic opportunity and the realization of human rights."

Indeed, the Obama administration's cyberspace-policy guidelines stressed the value of the Internet in the global economy and aimed to balance openness with privacy protection and security. It was in this same spirit that global leaders developed the new Internet policies, Weitzner and Kornbluh said.

Among policies listed in the communique are to promote and protect the global free flow of information on the Internet and to maintain the open, distributed, and interconnected nature on which the World Wide Web was built.

Other policies communicated by the group with the hopes they will be adopted globally include: ensuring transparency, fair process, and accountability; cooperating in a joint Internet policy development process that takes various stakeholders into account; strengthening consistency and effectiveness in privacy protection; promoting creativity and innovation; developing capacities to bring publicly available, reliable data into the policy-making process; strengthening consistency and effectiveness in privacy protection at a global level; and fostering voluntarily developed codes of conduct for Internet behavior.

# US and Russia Among 22 Nations Supporting International Cyber Resolution

## U.S. and Russia among 22 nations supporting international cyber resolution

BY ALIYA STERNSTEIN 07/05/2011

Russia and the United States are co-sponsoring a resolution to pre-empt cyberattacks that an influential international body is expected to adopt this week, according to a Belgium parliamentary member who introduced the decree. The proposal calls for member nations to exchange information about the way they intend to deploy cyber technology during military conflicts.

Russian support is notable because the former Soviet republic was blamed in 2007 for knocking out Internet access in neighboring Estonia. Both nations belong to the 56-member Organization for Security and Cooperation in Europe. OSCE parliamentarians are gathering this week in Serbia to select provisions for inclusion in the Belgrade Declaration, an annual statement that guides OSCE decisions. The organization, which represents North America, Europe and Central Asia, provides a venue for negotiations on conflict prevention and post-war rehabilitation.

"One advantage of OSCE is that we have Russia as a state," Belgian Parliamentarian Francois Xavier de Donnea told *Nextgov* in an interview Tuesday. "It is a place where the American and European countries can dialogue with the former Soviet Union and risks can be reduced."

Alexander Kozlovsky, deputy chairman of the Russian State Duma International Affairs Committee, signed the proposed provision, according to de Donnea.

"I think such a resolution could get unanimous support," de Donnea said.

Last month, defense ministers at NATO, which does not include Russia, approved a new policy on cyber defense to help allies protect their communications systems and deter cyberattacks.

Deputy Secretary of Defense William J. Lynn III said shortly after passage, "NATO is unanimous in acknowledging the need to elevate its treatment of network security," adding that the new strategic concept the alliance adopted last November "names cybersecurity as a leading priority for NATO in the 21st century."

But De Donnea said the ideal forum for worldwide discussion of cybersecurity threats is the United Nations.

"If the OSCE succeeds in conducting dialogues between states on norms in cybersecurity. . . it would be a major step toward a more global approach, which would be promoted by the United Nations," he said. The U.N. and OSCE do not share a budget but coordinate closely on field

operations.

Last week, Homeland Security Secretary Janet Napolitano said she believes the OSCE can play a meaningful role in forming international measures for state behavior in cyberspace, but she was not specifically addressing the resolution at the time, aides said Tuesday.

"We welcome consideration of the establishment of a cybersecurity unit within the OSCE secretariat with existing resources and look forward to discussing this in more detail with other OSCE participating states and partners," she said during remarks at a joint meeting of the OSCE Permanent Council and OSCE Forum for Security Cooperation in Vienna.

Separately, the White House in May distributed a voluntary international strategy for cybersecurity that, like the OSCE proposal, urges cooperation in developing standards for acceptable conduct on the Internet.

# Judge Rules Against Google in Street View 'Wi-Spy' Lawsuit

Judge rules against Google in Street View 'Wi-Spy' lawsuit
by Gregg Keizer, Computerworld Jul 4, 2011 11:35 am

*Editor's Note: This story is excerpted from Computerworld. For more Mac coverage, visit Computerworld's Macintosh Knowledge Center.*

*A federal judge has declined to dismiss charges against Google that it allegedly violated the Federal Wiretap Act when it collected personal data from Wi-Fi networks.*

U.S. District Court Judge James Ware on Wednesday tossed accusations that Google's Street View vehicles broke several states' laws when they harvested usernames, passwords and emails from consumers' and businesses' wireless networks, but allowed the claim that the company violated federal law to continue.

Google's Street View vehicles began cruising American roads in 2007 as part of the company's mapping program. Along with snapping photographs of each street and collecting GPS data, the vehicles also mapped the location of Wi-Fi networks to build a database that could be accessed by mobile devices to determine users' whereabouts.

Google acknowledged the privacy problem in May 2010, but said collection of personal data from Wi-Fi hotspots had been inadvertent. The company blamed an unnamed engineer for adding code to the Wi-Fi location detection software.

Although Google initially said that the packet sniffer grabbed only data fragments, it later acknowledged that the vehicles had harvested complete usernames and passwords from unprotected wireless networks, as well as emails.

To arrive at his ruling, Ware threaded his way though years of legislative history of federal privacy laws related to over-the-air communications, and even went to the Oxford English Dictionary in an attempt to define "radio communications."

He concluded that the exemptions built into the Federal Wiretap Act did not apply to

Google's snooping.

"The Court finds that Plaintiffs plead facts sufficient to state a claim for violation of the Wiretap Act," Ware wrote in his ruling. "Defendant's contention that Plaintiffs fail to state a claim for violation of the Wiretap Act, as Plaintiffs plead that their networks were 'open' and 'unencrypted,' is misplaced."

Jim Dempsey, the vice president for public policy at the Center for Democracy and Technology (CDT), a Washington D.C.-based advocacy organization, said that intercepting data communications from a Wi-Fi network, even one unsecured with a password, "should certainly be illegal."

But he also argued that Congress needed to clarify the law. "It's certainly far preferably to clarify the statute legislatively," Dempsey told Computerworld on Friday, rather than require judges like Ware to parse the ambiguous and outdated language of the 25-year-old Electronic Communications Privacy Act (ECPA). "But whichever way this case comes out, clarifying the statute on this particular point is not going to be easy."

Google said it was considering its next move.

"We believe these claims are without merit and that the Court should have dismissed the Wiretap claim just as it dismissed the plaintiffs' other claims," a Google representative said in an emailed statement today. "We're still evaluating our options at this preliminary stage."

However, a trade group co-sponsored by Microsoft, eBay, Intel, Oracle and others applauded Ware's ruling.

"Google has been a bad actor in our industry when it comes to privacy," Jonathan Zuck, the president of the Association for Competitive Technology (ACT), said by email Thursday. "We have long been aware of the negative impact Google has had on consumers' faith in the security of their online privacy. It is our hope that the courts

continue to treat the Wi-Spy matter seriously so consumer confidence may be restored."

"Wi-Spy" is the name some, including ACT, have pinned on the Street View debacle.

ACT has regularly voiced anti-Google opinions when the search giant has been in legal hot water. Last week, for example, the group said it supported the Federal Trade Commission's (FTC) investigation into possible antitrust violations by Google, saying, "Government intervention in the case of Google is what is best for the technology space" and calling the Microsoft rival's behavior "reckless."

Ironically, the ACT was a very vocal backer of Microsoft when the company was accused by European Union antitrust regulators of abusing its monopoly position.

Ware also dismissed the plaintiffs' charges that Google violated California business practice laws, but gave the plaintiffs until Aug. 1 to amend their complaint.

The demand by the 22 plaintiffs that their lawsuit be granted class-action status is still pending.

"This is just another in a whole long series of cases that, case after case, show that the ECPA is a complicated statute that's very hard to understand," said Dempsey of the CDT. "Congress needs to respond."

# Agencies Face Challenges Developing Systems for Multiple Mobile Operating Systems

## Agencies face challenges developing for multiple mobile operating systems

June 27, 2011 — 9:26am ET | By Molly Bernhart Walker

As soon as the Environmental Protection Agency decided it would begin developing public-facing mobile applications, Dalroy Ward, senior technology advisor at EPA's office of information analysis and access, made a visit to the agency's ethics officer.

"They very simply said, 'You can't do something just for one device, one network,'" said Ward, while speaking June 23 at an AFCEA Bethesda event. "That could be perceived as an endorsement that's going to go out to the public."

At the same time, said Ward, agencies can't afford to build and support mobile operating systems that only claim 1 percent of the market. Ward watches market penetration data for the various mobile operating systems very closely, as it dictates what the agency will develop for and support.

"At the very minimum we have been doing iOS, Android and a mobile web, so that any relatively smart phone--that's not a smartphone but that can just handle a web browser--can do our mobile applications," said Ward.

But even if an agency commits to building apps for the three, leading mobile OSes it will likely struggle with variations to the user experience, introduced by carriers and manufacturers, said Lt. Col. Anmy Torres, director of defense knowledge online and secure go mobile at the Defense Information Systems Agency.

"Each device is different. You get Android 2.3 on a device and you think you developed something that works but the manufacturer has put in a few other features or things and the carrier has a different flavor of the device and you've got to work with that," warned Torres.

Torres focuses on internally-facing mobile applications that help employees and service members do their jobs more effectively and efficiently. Despite a longstanding allegiance to BlackBerry devices at DoD, Torres said her shop is "customer driven," and the demand iPhones, iPads and Android devices is increasing.

The recurring question for Torres is: "What are the security requirements we need to address and put in place in order to adopt new devices?" said Torres.

Many times, she said, DISA has successfully enabled remote wiping, common acces card compliance, and disabled GPS, WiFi and cameras, through security applications provided by third-party software vendors.

"We have [to have] a way to secure it that is painless for everybody, not just for the customers but also for the people who are supporting--the system administrators behind the scenes making sure that everything works on their device," said Torres.

Earlier in the week, the General Service Administration's office of citizen services and innovative technologies announced a new project called "Making Mobile Gov." During the first phase of the initiative OCSIT plans to assist agencies in educating leadership on the benefits of a consumer-focused mobile strategy. OCSIT will also help agencies develop criteria for project selection, encourage investment in mobile and facilitate interagency collaboration around mobility. Eventually, OCSIT will launch a community-generated wiki around the effort.

EPA recently launched an "Apps for the Environment" contest which asks mobile application developers to create "data mashups" from data sets released by EPA and the Department of Health and Human Services. Ward touted the interagency collaboration and said the agencies' data can be brought together in ways that "allow the public to draw their own conclusions."

"It's potentially very powerful and potentially very dangerous, because just because there's a concentration of a chemical that does not necessarily mean it's causing some disease, but there are some really cool things that can be done," added Ward.

# Are We Ready For the Era of .Anything?

Tuesday, June 28, 2011

**Are We Ready for the Era of .Anything?**
New top-level domains will open up new possibilities but could cause confusion.
By David Talbot
Today's narrow range of so-called top-level domains (such as .com and .org) are about to be joined by an unlimited range of new ones. These could be used as corporate branding (.coke or .pepsi, for example), to organize multiple sites into categories (think .food, .bank, and anything else). But, while they could open new commercial opportunities and have some security benefits, the domains could also confuse some users, creating new opportunities for fraud artists.

For decades, the Internet has operated with just 21 top-level domains—the most common one being .com (which has about 200 million registered domain names)—plus country names like .jp for Japan and .de for Germany. But last week, the Internet Corporation for Assigned Names and Numbers (ICANN), the nonprofit body that governs the naming system, decided after years of discussion to allow the new custom top-level domains. The organization is about to launch a campaign to raise awareness about their availability, and will accept applications starting January 12, 2012.

Some companies are already lining up. The camera company Canon, for example, has said it will apply for ".canon" to create one central site, so users wouldn't need to type "canon.com" in the United States, "canon.de" in Germany, and so on. Some global organizations might want to do the same, for similar reasons. Indeed, ICANN expects most applicants to be corporations. The new top-level domains will work in non-Latin alphabets, too.

ICANN says it expects the new domains to usher in new forms of marketing and, in some cases, to add a level of security. For example, a specialized top-level domain such as .bank might be secured with domain name security called DNS-SEC—which verifies that a domain name seen by a user corresponds to the numerical computer address assigned to a bank's servers. This would require an additional vetting process for any company that applied for a .bank domain name. But then users could feel particularly confident that the site they are viewing is legitimate.

However, some observers expect the domains to introduce confusion—and perhaps some new security risks. User confusion already plays a key role in the success of many online scams, such as phishing, in which fraudulent websites that look like bank sites—and that have domain names that seem right—coax people into entering their account numbers. (Similarly, billion-dollar frauds like fake antivirus scams thrive in part

on confusion about what a correct virus warning should look like.)

So in theory, scam artists could register something like .savingsbank and confuse people. "You can probably imagine that if someone registers .wellsfargobank and customers erroneously try to go to http://wellsfargobank/; then the end user customer is maybe not going to get the 'wellsfargobank' they thought they were asking for," says Paul Vixie, chairman and chief scientist of Internet Systems Consortium, a nonprofit developer of Internet software and protocols.

There is a limiting factor on such concerns, of course; would-be creators of new top-level domains will have to fork over $185,000 and go through a bureaucratic process to win approval, notes Richard Lamb, who is in charge of domain-name security deployment at ICANN. By contrast, it's far easier to set up a similar domain name—say, wellsfargobanc.com—to fool people. But the consensus of ICANN's board is that the overall security risks of the new effort are low. The details of their discussions can be found here.

But Lamb adds that glitches might arise if users try to reach new top-level domains without typing any dots—such as http://canon or similar addresses.

Some operating systems will first look to see if "canon" exists as part of the local domain (for example: canon.technologyreview.com) and then send you there. Similar problems could pertain to e-mail systems. "Fresh from the meeting floor this week, there have been discussions about how the lack of dots in the new top-level domains may get misinterpreted by existing software," Lamb said.

Either the new top-level domains will need to be preceded by dots, or software will have to change.

The process that led to the new top-level domains was years in the making, and involved the full range of Internet participants from around the world: governments, businesses, technology experts, and end users.

Steve Crocker, vice chair of ICANN's board of directors and an architect of the Internet's original protocols, says it will be fascinating to see how all of these participants adopt and react to new top-level domains. "I hope that this is studied in business schools going forward and analyzed in many ways," he said in his remarks last week. "And we'll look back and try to understand what the results were compared to what we expected."

# Are We Ready For the Era of .Anything?

# World's Data Will Grow by 50X in Next Decade, IDC Study Predicts

World's data will grow by 50X in next decade, IDC study predicts

IT execs will likely have trouble finding enough people with the skills and experience to manage it, analysts say

**Lucas Mearian**

**June 28, 2011** (Computerworld)

In 2011 alone, 1.8 zettabytes (or 1.8 trillion gigabytes) of data will be created, the equivalent to every U.S. citizen writing 3 tweets per minute for 26,976 years. And over the next decade, the number of servers managing the world's data stores will grow by ten times.

Those are some of the findings in the fifth annual IDC Digital Universe study that was released today.

Interestingly, the amount of data people create by writing email messages, taking photos, and downloading music and movies is minuscule compared to the amount of data being created about them, the EMC-sponsored study found.

The IDC study predicts that overall data will grow by 50 times by 2020, driven in large part by more embedded systems such as sensors in clothing, medical devices and structures like buildings and bridges.

# World's Data Will Grow by 50X in Next Decade, IDC Study Predicts

IDC Digital Universe study.

The study also determined that unstructured information - such as files, email and video - will account for 90% of all data created over the next decade.

The bad news: the number of IT professionals available to manage all that data will only grow by 1.5 times today's levels, IDC said.

The number of people with the skills and experience to manage the fast-growing stores of corporate simply isn't keeping pace with demand, IDC noted.

The study also notes that data security will continue to be a key issue for IT managers.

For example, though 75% of data today is generated by individuals, enterprises will have some liability for 80% of it at some point in its digital life. And less than one-third of all stored data today has even minimal security or protection; only about half the information that should be protected is protected at all, IDC stated.

The good news: new hardware and software technologies have driven the cost of creating, capturing, managing and storing information down to one-sixth of what it was in 2005.

For example, data deduplication and compression technologies have reduced the amount of data transmitted across networks and stored in data centers, while virtualization and thin provisioning (allocating just enough disk array capacity to store data) have increased storage system utilization rates.

"As an industry, we've done a tremendous job at lowering the cost of storing data. As a result, people and companies store more data," said David Reinsel, IDC's vice president of storage and semiconductor research.

Since 2005 annual investments by enterprises in hardware, software and cloud services technologies, along with the staff to manage information, has increased 50% to $4 trillion.

New data capture, search, discovery, and analysis tools will also create data about data automatically, much like facial recognition routines that help tag Facebook photos. Data about data, or metadata, is growing twice as fast as the digital universe

as a whole. A gigabyte of stored data can use as much as a petabyte of information, according to Reinsel.

"So, the 1.8 zettabytes includes both what we store and what we don't store. Think about watching a YouTube video or HD movie over cable or satellite," Reinsel said.

For example, during a consumer's "consumption" of information, while watching a movie or YouTube video, metadata is created but not necessarily stored, or is stored for only a few milliseconds.

Currently, cloud computing accounts for only 2% of IT spending. By 2015, though, close to 20% of all information will be attached to cloud services some way, and as much as 10% will reside in a cloud infrastructure, IDC stated.

The next step, Reinsel said, is to enable companies to better extract value out of their mountains of data, via big data analytics.

"This is where real opportunities lie, and where some folks may miss the boat. As soon as big data success stories are advertised and people see that there is gold in their data ... then you will find more companies desiring to put more data online," he said.

But if all a company does is keep storing more data, and are unsuccessful at finding the gold in it, then there will be little if any return on investments in storage and management technology, he added.

# 'Geeky' World of IT Loses Its Appeal as a Career Choice

'Geeky' world of IT loses its appeal as a career choice
By Maija Palmer
Published: 06:52am Jul 06, 2011

There are a host of powerful women in the top echelons of internet companies, including Carol Bartz, chief executive of Yahoo, Sheryl Sandberg, chief operating officer at Facebook, and Marissa Mayer, vice-president of location services at Google. But they remain something of an anomaly. Women account for just 6 per cent of the chief executives of the top 100 technology companies in the US, and just 22 per cent of the IT workforce overall, according to the National Center for Women & Information Technology. None of the UK's most prominent listed technology companies are run by a woman.

What is more, the participation of women in technology appears to be falling. In the UK, women accounted for just 18 per cent of technology professionals in 2010, down from 22 per cent in 2001.

"I am surprised that the statistics aren't moving upwards," says Wendy Tan White, founder and chief executive of Moonfruit, a UK-based technology start-up. "If you look at Facebook, Groupon and Zynga, some of the fastest-growing technology companies at the moment, most of the customer base is female. It is one of the most fertile times for women to get involved in technology."

Overt sexism or discrimination does not appear to be the problem. "There is nothing institutional that is stopping women. It is not misogynistic," says Alicia Navarro, founder of Skimlinks, an online advertising technology company.

It was never difficult being one of the rare women on her university computer science course or at technology companies, she says. "In my

experience, geeks have always been very welcoming of there being more girls in their midst."

However, a culture of long hours and an image of "geekiness" were some of the key concerns raised by women surveyed by Intellect, the trade body for UK technology companies, earlier this year.

Juliet Tzabar, chief executive of Plug-In Media, a digital media production company, acknowledges that she would find it hard to balance family life and a technology job if she did not run her own company. "I can pick up my kids from school two or three times a week," she says. "It is very finely balanced, but it works. I am not sure I would be able to do that as an employee."

Carolyn Everson, vice-president of global marketing solutions at Facebook, says: "These are difficult jobs; there is a lot of travel and responsibility. Finding ways to balance that [with family life], some women have a difficult time."

Many of the highest-ranking female IT specialists tend to be found either at start-ups or at non-technology companies. The chief information officers of the BBC, the Metropolitan Police and Network Rail in the UK are women.

The biggest problem is that young women are not entering the profession in sufficient numbers. In the UK's further education system, only 9 per cent of computer science students are female, down from 14 per cent a decade ago. In the US, just 18 per cent of undergraduate computing degrees in 2009 were awarded to women; in 1985, women earned 37 per cent of those degrees.

"It is fundamentally about getting them in younger," says Ms Tan White. "We have to take away the image that it is too geeky."

Karen Price, chief executive of e-skills UK, which promotes technology learning in the UK, says old-fashioned university courses might be to blame.

"A lot of employers believe that our computer science degrees tend not to deliver the type of employees they need," she says. "I wonder if the traditional curriculum of these courses is reinforcing stereotypes and female interest is quickly turned off by university."

To combat this, e-skills UK has supported the creation of a new IT and business management university degree, to broaden the appeal of technology.

It also launched a programme called Computer Clubs for Girls (CC4G) six years ago to get schoolgirls interested in technology. However, commitment to the scheme was patchy. It was later widened to include boys and lost most of its girl participants, and e-skills UK will attempt to relaunch it as an all-girl initiative in September.

Kerry Benford is proof that these programmes can succeed. She was inspired to study IT after joining the CC4G scheme run by her school at age 13. "It showed me that you don't have to do binary coding to work in IT," she says. "You can look at the business side. IT supports every field at work."

Ms Benford went on to complete one of the newly created IT and business management university degrees and is now a graduate trainee at PwC, the professional services company. "I haven't felt held back yet," she says.

Yet as an attractive, petite blonde, she feels she still has to fight against stereotypes. "People are always surprised that I have done an IT degree," she says. "They expect me to have done media studies. I don't know if that is because I am a woman, but I get that a lot."

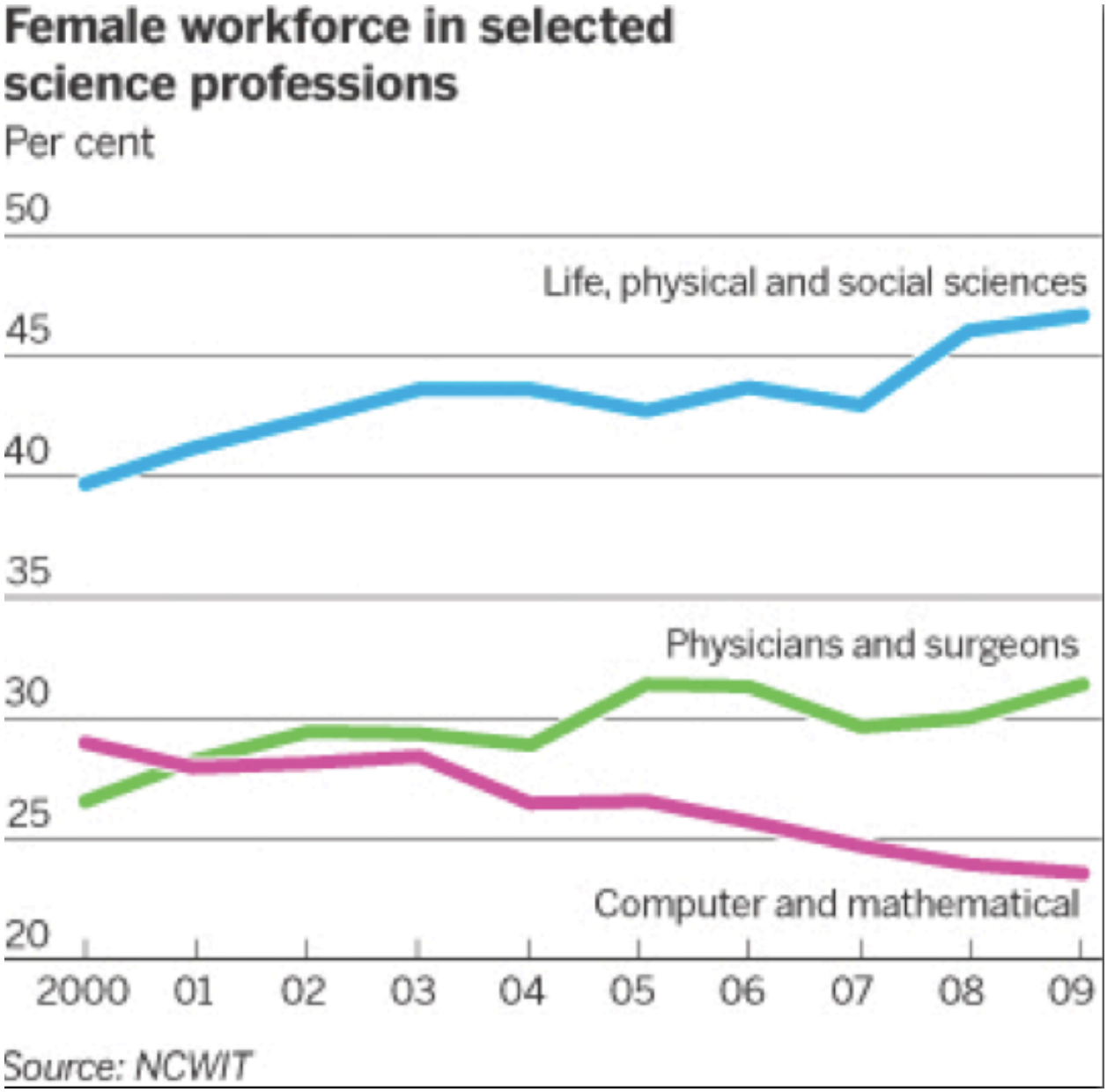
Mentoring and networking organisations for women have sprung up, such as Change the Ratio, a New York-based organisation for women entrepreneurs. There are also Girl Geek Dinners, a networking organisation started in London that has spread worldwide; Girls 'n' Gadgets, a technology website

for women, run by women; and Womenintechnology.co.uk, which runs events, training courses and a jobs board for Britain's female technologists. Illuminate Ventures, a US-based investment firm, backs many female entrepreneurs, largely on the premise that teams with gender diversity tend to outperform. According to the National Center for Women & Informaton Technology, tech companies with more women on their management teams have a 34 per cent higher return on investment.

However, IT is still seen as an industry in desperate need of a better image. "It is a question of good PR," says Ms Navarro. "It is competing with subjects such as media studies, PR and marketing, which seem much more exciting. We need more articles about how fantastic it is to be a product manager at an IT company. I think it is the best job in the world, but it needs to be glamorised."

*View a chart displaying the proportion of the female workforce in selected science professions*

# 'Geeky' World of IT Loses Its Appeal as a Career Choice



## Storage Wars: Web Growth Sparks Data-Center Boom

By ANTON TROIANOVSKI

For years, as Internet use boomed, builders of the giant, air-conditioned computer warehouses known as data centers couldn't keep up with demand.

View Full Image

Reuters

Apple's Steve Jobs in San Francisco before an image of the server farm that the company unveiled in North Carolina last month.

Now, though many investors continue to pile into the data-center business, one of the few hot spots in real estate, others fear the peak may be past.

In key markets from New Jersey to Silicon Valley, there are signs that supply is catching up with the needs of the telecommunications, Internet and other companies that rent space from data-center landlords. Adding to the concern, some large tenants, such as Facebook Inc., are building their own facilities and avoiding paying rent to outside developers.

In the San Francisco Bay Area, rates charged to big tenants who rent entire data centers or large parts of them have fallen some 20% in the past year and a half, amid a burst of new supply, says Tom Ray, chief executive of CoreSite Realty Corp., a data-center landlord with facilities in the area.

Other market participants say they haven't seen a steep decline in Bay Area rates, but some are nervous about a new wave of construction expected to hit the market later this year.

"A lot of people are going to get burned, because they've got caught in euphoria," says Manny Medina, a longtime data-center investor who in April sold his company, Terremark Worldwide Inc., to Verizon Communications Inc. for $1.4 billion. "Eventually, there's going to be a reckoning."

Data centers, which house and link the servers and other gear that form the backbone of the Internet, have become a big business. Revenue for providers in North America will reach $8.1 billion this year, up from $5.7 billion in 2009, according to Tier1 Research, which tracks the industry.

Terremark now has nearly 50 data centers. Kerry Bailey, who runs Terremark for Verizon, says the telecom giant's ability to integrate new facilities into its global network sets its services apart in an increasingly crowded field. "We believe the market is moving in our direction," Mr. Bailey said.
Many data-center developers, who often break ground before signing up tenants, are continuing to steam full-speed ahead. Their theory: with Internet traffic exploding— Cisco Systems Inc. expects it to quadruple over the next five years— and more companies outsourcing their data storage, demand for the space can't help but increase.

In Silicon Valley and the New York metropolitan area, the supply of data-center space rose by just 3% in 2009 but is expected to grow by nearly 10% this year as real-estate financing opens up, according to Tier1.

Digital Realty Trust Inc., a major data-center developer, had more than 1 million square feet under construction in 11 markets from Boston to Singapore as of March 31, at a cost it estimated at $321 million. Another developer, DuPont Fabros Technology Inc., had three massive projects under way in California, Virginia and Illinois at a cost of around $550 million.

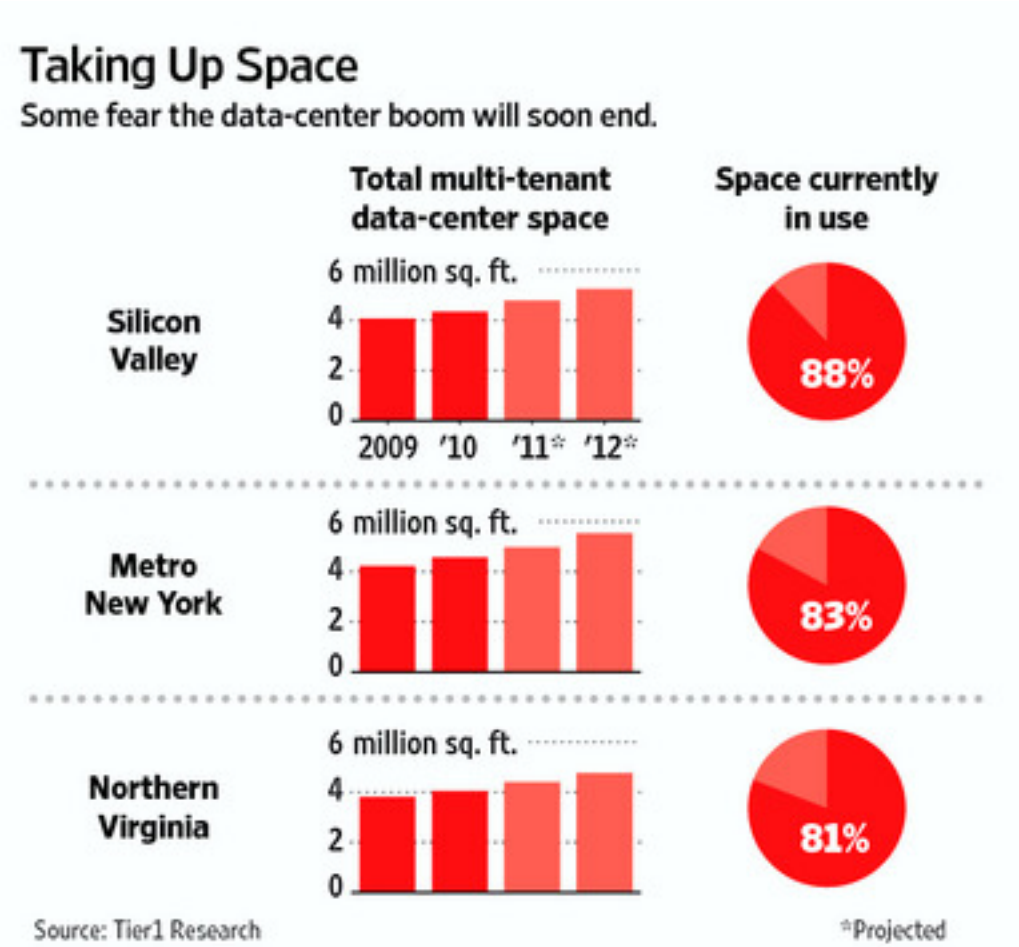
Vantage Data Centers, owned by private-equity firm Silver Lake Partners, is building a 314,000 square-foot, $300 million complex in Silicon Valley and planning to expand to other parts of the country.

"The amount of capital going into data-center construction is remarkable," says Stephen M. Smith, CEO of data-center operator Equinix Inc. This year alone, Equinix, which runs 98 data centers, has set plans to build or open new facilities in Amsterdam, Paris, Dallas, New York and near São Paulo, Brazil.
Equinix plans to spend $615 million to $665 million in 2011 on capital projects, primarily data-center expansion. But even Mr. Smith says overbuilding in the industry "is a main concern."

In New Jersey, major data-center space—properties 100,000 square feet or larger—

has roughly doubled since 2005, according to commercial-real-estate firm CB Richard Ellis Group Inc. That helped push the vacancy rate in the northern part of the state to what KeyBanc Capital Markets estimates was 14% in April, up from 12% in December. In the Bay Area, CoreSite expects new supply to outpace demand by as much as 50% in the second half of the year.

One reason for the imbalance: Facebook, a huge user of data centers, has been building its own sprawling server farms, joining other tech giants that already operate their own facilities. Google Inc. has been building its own data centers for years, while Apple Inc. unveiled a new data center in North Carolina last month.




"It used to be a no-brainer: You build it, and if it's well built and well located, Facebook would lease it," says Sutton Roley, a Silicon Valley data-center broker with brokerage firm Cassidy Turley. "That's no longer the case."

Some who had predicted trouble in the industry in recent months say demand is holding up better than they had expected. Ross Nussbaum, an analyst who follows real-estate stocks for UBS AG, published a research note in December warning data-center developers were trading at "unsustainably high valuations" despite slowing

growth, rising competition and pricing pressure.

Yet so far this year, shares of the largest data-center real-estate investment trust, Digital Realty, are up 24%, outpacing the 11% gain in a Dow Jones index of real-estate stocks.

"The market has chosen to look past the increased level of supply that has entered some markets," Mr. Nussbaum says. He says he still believes Digital Realty's valuation is unsustainable.

A Digital Realty spokeswoman said supply and demand are "pretty much in balance" in two of the company's key markets—Santa Clara, Calif., and New Jersey—but it still sees opportunity in other markets, such as Boston, and overseas.

—Spencer E. Ante contributed to this article.

**Spy Geeks Want Holodeck Tech for Intel Analysts**

- By Adam Rawnsley July 7, 2011 | 6:47 pm

The holodeck: a room that can create an interactive 3-D hologram of just about any environment you can think of. It's been the dream of Star Trek nerds ever since *The Next Generation* debuted on TV. Well brace yourself, Trekkies, and try not to soil those Starfleet unitards in glee. The U.S. intelligence community had heard your prayers and is now taking a step towards building its own holographic simulator.

Iarpa, the intelligence community's advanced research outfit, announced this month that's it's embarking on a Synthetic Holographic Observation (SHO) program, a quest to build a system that lets intel analysts collaborate with each other using interactive 3-D holographic displays.

Before you get too excited, SHO isn't going to be an exact replica of the holodeck. Instead of a geometrically patterned room on board the *Enterprise*, the holograms will come from workstations here on earth. While Iarpa's announcement promises "dynamic, color, high-performance" holograms, the all-around holographic environment that's indistinguishable from reality is still a long ways off. In the meantime, Iarpa's program will rely on synthetic, electronically reproduced light fields.

SHO is bringing part of the holodeck concept one small step closer to reality, though. The program is aimed at generating 3-D displays that let analysts get a better feel for the mountains of imagery that the intelligence community collects. In particular, SHO needs to render conventional imagery and LIDAR (light detection and ranging) into holographic light fields. LIDAR bounces beams of light off objects in a manner not too different from conventional radar, allowing users to quickly make 3-D images and maps.

Just generating a hologram from aerial imagery isn't enough, though. SHO needs to be able to let multiple analysts work together on the same image at the same time. To do that, it has to be interactive. Iarpa's asking prospective builders to make a hologram that analysts can navigate and manipulate in ways that regular maps don't allow.

This isn't the defense world's first foray into the world of holograms. Some projects, like the "Face of Allah," have aimed at beaming a 3-D image of a deity over the battlefield in hopes of striking fear of the divine into the hearts of the enemy. Darpa's contract with Vuzix of Rochester, New York is a little closer to SHO's goals. Vuzix is building eyewear that would give troops on the ground a holographic image of nearby air assets and allow them to call in airstrikes with greater precision.

Unlike the battlefield hologlasses, eyewear-based devices need not apply for SHO. Iarapa wants its holographic displays to be visible to the naked eye.

Analysts' eyeballs are a special concern for IARPA, too. Conventional 3-D technology can lead to eye strain when used for long periods of time. Iarpa needs analysts to use SHO for long periods of time so those pitching a holographic system need to make systems that are easy on the eyes over extended use.

Iarpa's announcement provides a few examples of how they'd like to use their holographic system. During the testing phase, it wants to see how holograhic systems work on LIDAR data of urban environments and terrain, and conventional imagery of buildings and airspace.

But for a more real-life example of how holographic displays could be useful, take the bin Laden raid as a test case. In that instance, the intel community's imagery nerds used satellites and airborne sensors to snap all kinds of imagery of the terror leader's Abbotabad crib. That imagery helped Navy SEALs build a real life mockup of Chez bin Laden at Bagram Air Field. And it may have led the National Geospatial Intelligence

Agency — the intel community imagery exploitation shop — to make virtual models of the compound with its software.

If SHO can move past the prototype phase, imagery analysts would be able to quickly generate immersive models of a high-value target's lair. Multiple analysts and personnel could take a virtual stroll through the building and help plot a raid without ever having to visit the real-world replica.

# Why Lithium Ion Batteries Die So Young

Why lithium-ion batteries die so young

By Josie Garthwaite Jun. 29, 2011, 12:00am PT 5 Comments

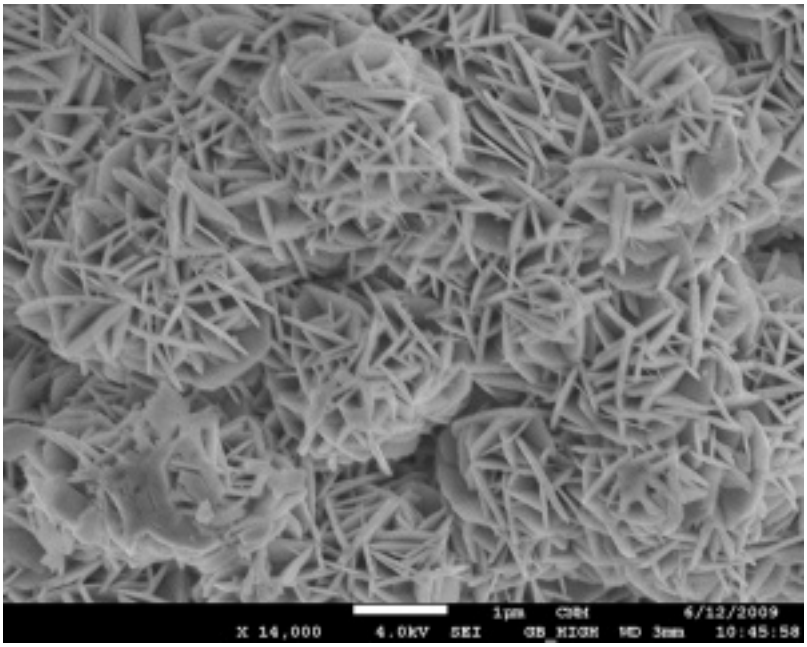
The death of a battery: We've all seen it happen. In phones, laptops, cameras and now electric cars, the process is painful and — if you're lucky — slow. Over the course of years, the lithium-ion battery that once powered your machine for hours (days, even!) will gradually lose its capacity to hold a charge. Eventually you'll give in, maybe curse Steve Jobs and then buy a new battery, if not a whole new gadget.

But why does this happen? What's going on in the battery that makes it give up the ghost? The short answer is that damage from extended exposure to high temperatures and a lot of charging and discharging cycles eventually starts to break down the process of the lithium ions traveling back and forth between electrodes.

The longer answer, which will take us through a description of unwanted chemical reactions, corrosion, the threat of high temperatures and other factors affecting

performance, begins with an explanation of what happens in a rechargeable lithium-ion battery when everything's working *well*.

**Lithium-ion battery 101**




In a typical lithium-ion battery, we'll find a cathode, or positive electrode, made out of a lithium-metal oxide, such as lithium cobalt oxide. We'll also find an anode, or negative electrode, which today is generally graphite. A thin, porous separator keeps the two electrodes apart to prevent electrical shorting. And an electrolyte, made of organic solvents and lithium-based salts, allows for the transport of lithium ions within the cell.

During charging, an electric current forces lithium ions to move from the cathode to the anode. During discharging (in other words, when you use the battery), ions move back to the cathode.

Daniel Abraham, a scientist at Argonne National Laboratory leading research into how

lithium-ion cells degrade, compared this process to water in a hydropower system. Moving water uphill requires energy, but it flows downhill very easily. In fact, it delivers (kinetic) energy, said Abraham. Similarly, a lithium cobalt oxide cathode “does not want to give up its lithium,” he said. Like moving water uphill, it requires energy to take lithium atoms out of the oxide and load them into the anode.

During charging, ions are forced between sheets of graphene that make up the anode. But as Abraham put it, “they don’t want to be there. When they get a chance, they’ll move back,” like water flowing downhill. That’s discharging. A long-lasting battery will survive several thousand of these charge-discharge cycles, according to Abraham.

**When is a dead battery really dead?**

When we talk about “dead” batteries, it’s important to understand two performance metrics: energy and power. For some applications, the rate at which you can get energy out of the battery is very important. That’s power. In electric vehicles, high power enables rapid acceleration and also regenerative braking, in which the battery needs to

accept a charge within a couple of seconds.

In cell phones, on the other hand, high power is less important than capacity, or how much energy the battery can hold. Higher-capacity batteries last longer on a single charge.

Over time the battery degrades in a number of ways that can affect both power and capacity until eventually it simply can't perform its basic functions.

Think of it in terms of another water analogy: Charging a battery is like filling a bucket with water from a tap. The volume of the bucket represents the battery's energy, or capacity. The rate at which you fill it — turning the tap on full blast or just a trickle — is the power. But time, high temperatures, extensive cycling and other factors end up

creating a hole in the bucket (dear Liza, dear Liza . . .).

In the bucket analogy, water leaks out. In a battery, lithium ions are taken away, or “tied down,” said Abraham. Bottom line, they’re prevented from going back and forth between the electrodes. So after a few months, the cell phone that initially required a charge only once every couple of days now needs a charge every day. Then it’s twice a day. Eventually, after too many lithium ions have been tied down, the battery won’t hold enough of a charge to be useful. The bucket will stop holding water.

Why does this happen? Well, in addition to the chemical reactions that we want to happen in the battery, there are also side reactions. Barriers arise that impede the motion of lithium ions. So the electric car that went, say, zero to 60 in 5 seconds off the lot will take 8 seconds after a few years, and maybe 12 seconds after 5 years. “All the energy is still there, but it can’t be delivered fast enough,” said Abraham. The ions run into roadblocks.

**What breaks down and why**

The active portion of the cathode (the battery's source of lithium ions) is designed with a particular atomic structure, for stability and performance. When ions are removed, sent over to the anode and then inserted back into the cathode, we ideally want them to return to the same spot, in order to preserve that nice stable crystal structure.

The problem is that the crystal structure can change with each charge and discharge. An ion from apartment A doesn't necessarily come home but could instead insert herself into apartment B next door. So the ion from apartment B finds her place occupied by this drifter and, not being one for confrontation, decides to take up residence down the hall. And so on.

Gradually these "phase changes" in the material transform the cathode to a new crystal structure with different electrochemical properties. The particular arrangement of atoms, which enabled the desired performance in the first place, has been altered.

In hybrid vehicle batteries, which only need to provide power when the vehicle is accelerating or braking, noted Abraham, these structural changes occur much more slowly than in electric vehicles. This is because only a small fraction of lithium ions in the system move back and forth in any given cycle. As a result, he said, it's easier for them to return to their original locations.

**Problem of corrosion**

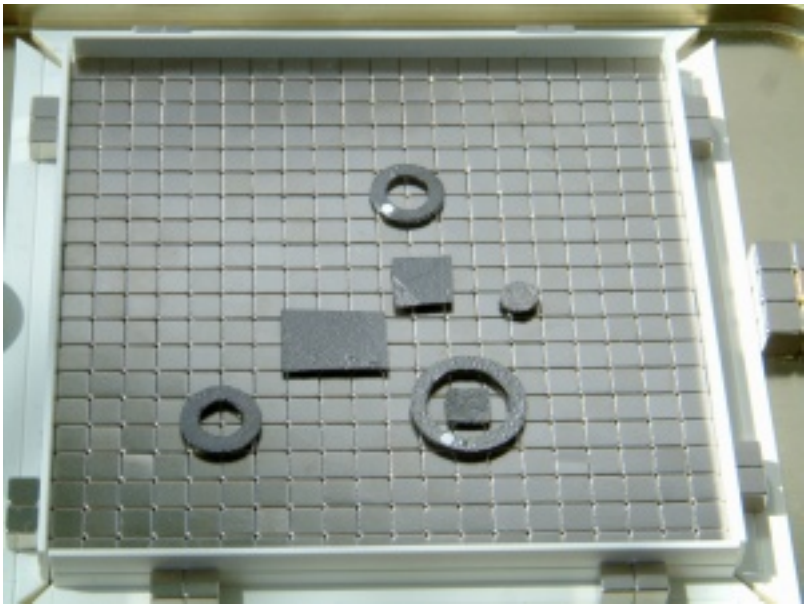
Degradation can occur in other parts of the battery as well. Each electrode is paired with a current collector, which is basically a piece of metal (typically copper for the anode, aluminum for the cathode) that gathers electrons and moves them to an external circuit. So you have slurry made from an “active” material like lithium cobalt oxide (which is ceramic and not a very good conductor), plus a gluelike binder painted over this piece of metal.

If the binder fails, the coating can peel off the current collector. If the metal corrodes, it can’t move electrons as efficiently.

Corrosion within the battery cell can result from an interaction between the electrolyte and electrodes. The graphite anode is highly “reducing,” which means it *gives up* electrons easily to the electrolyte. This can produce an unwanted coating on the graphite surface. The cathode, meanwhile, is highly “oxidizing,” which means it easily *accepts* electrons from the electrolyte, which in some cases can corrode the aluminum current

collector or form a coating on the cathode particles, Abraham said.

**Too much of a good thing**



Graphite — the material commonly used to make an anode — is thermodynamically unstable in an organic electrolyte. What that means is that the very first time our battery is charged, the graphite reacts with the electrolyte. This forms a porous layer (called a solid electrolyte interphase, or SEI) that actually protects the anode from further attacks. This reaction also consumes a little lithium, however. So in an ideal world, we would have that reaction occur once to create the protective layer and then be done with it.

In reality, however, the SEI is a sadly unstable defender. It does a good job of protecting the graphite at room temperature, said Abraham, but at high temperatures or when the battery runs all the way down to zero charge ("deep cycling"), the SEI can partially dissolve into the electrolyte. (At high temperatures, electrolytes also tend to decompose and side reactions accelerate.)

When friendlier conditions return, another protective layer will form, but this will eat up more lithium, giving us the same problem we had with the leaky bucket. We'll have to recharge our cell phone more often.

Now, as much as we need that SEI to protect the graphite anode, there can be too much of a good thing. If the layer thickens too much, it actually becomes a barrier to the lithium ions, which we want to flow freely back and forth. That affects power performance, which is, as Abraham emphasized, "extremely important" for electric vehicles.

**Building better batteries**

So what can be done to make our batteries last longer? In the lab, researchers are looking for electrolyte additives to function like vitamins in our diet, enabling the battery to perform better and live longer by reducing harmful reactions between the electrodes and electrolyte, said Abraham. They're also seeking new, more-stable crystal structures for the electrodes, as well as more-stable binders and electrolytes.

Engineers at battery and electric car companies, meanwhile, are working on the battery pack and thermal management systems to try and keep lithium-ion cells within a constant, healthy temperature range. As consumers, the rest of us can avoid extreme temperatures and deep cycling, and for now keep grumbling about those batteries that always seem to die too soon.

*Images courtesy of Argonne National Labs, felixtsao, warrenski, MitchClanky2008, bizmac*

# Navy Orders Study on UCLASS Concepts

Navy orders study on UCLASS concepts

By Philip Ewing Monday, June 27th, 2011 2:30 pm

The Navy wants an Unmanned Carrier-Launched Airborne Surveillance and Strike aircraft — or UCLASS — to fly off its carrier decks by 2018, and to that end it has awarded Boeing a contract to study just how it can get there, the aerospace company said Monday. Basically, from Boeing's announcement, it sounds as though the Navy wants to lay down as much groundwork as possible to prove that it'll be possible to take an aircraft, get it out to sea, on the cat, into the air and then trap it back on board.

From Boeing's announcement:

Boeing has received a $480,000 study contract from the U.S. Navy to support pre-Milestone A activities including development of a concept of operations, an analysis of alternatives, and an investigation of potential material solutions for the Navy's Unmanned Carrier-Launched Airborne Surveillance and Strike (UCLASS) program.

"The Navy wants UCLASS in the fleet in 2018," said Jimmy Dodd, vice president, Advanced Boeing Military Aircraft. "Boeing has been delivering carrier-based aircraft to the Navy since 1925. With Boeing's broad experience in unmanned systems and rapid prototyping, and nearly 90 years of carrier-based aircraft know-how, we are prepared to meet that schedule to support the mission and requirements the Navy establishes. This contract is the start of that."

The UCLASS system will consist of an air segment, a connectivity and control segment, a Carrier Vessel-Nuclear (CVN) segment (launch and recovery), and a systems support segment. The work on the eight-month contract, according to the Navy's Broad Agency Announcement, will conceptually demonstrate that a UCLASS system can provide a persistent CVN-based Intelligence, Surveillance & Reconnaissance and strike capability supporting carrier air wing operations in the 2018 time frame.

There are those who wear the Navy Wings of Gold — and those who don't — who believe it's more trouble than it's worth to try to teach an unmanned aircraft to catch an arresting wire on an aircraft carrier, at least with today's technology. You won't be able to recover your UAVs as often and as predictably as you can recover human pilots, one argument goes, so there's a good chance that if tomorrow's carriers sail with squadrons of UAVs, they'll come home missing several unlucky birds that had to try to land at night or in rough weather.

Nonsense, say UAV advocates: It's only a matter of math and physics before an unmanned aircraft can land on a carrier as well or better than a human pilot. And besides, in tomorrow's anti-access environments, when warships are going to need to

keep ever-farther away from their targets, only UAVs will have the stealth, range, ability to loiter and other advantages that the Navy needs. In other words, boosters say, UAVs are the key to the future relevance of aircraft carriers. What Boeing's study will apparently investigate is how much of what each of these camps believes is right — and how much is wrong.

Not only that, it sounds like Boeing will be charged with coming up with the initial concepts and doctrines for how a carrier could use its UAVs. This has the potential to be very interesting: Suppose tomorrow's carriers could use their UAVs to guard against the dreaded small-boat swarm attack, first watching for bad guys and then attacking them at range, if needed, while the ship kept safely away. Or imagine a carrier being able to keep UAVs in the air constantly searching for enemy submarines, saving human crews until they needed to drop a torpedo on the target. Of course the UAVs could well take that job, too.

## Global race on to match U.S. drone capabilities

(William Wan/ THE WASHINGTON POST ) - In recent years, the Chinese have begun developing equivalents to some of the most advanced U.S. drones. The Pterodactyl, is the Chinese answer to the MQ-9 Reaper, one of U.S. Air Forces' most advanced armed drones.

By William Wan and Peter Finn, Published: July 4

At the most recent Zhuhai air show, the premier event for China's aviation industry, crowds swarmed around a model of an armed, jet-propelled drone and marveled at the accompanying display of its purported martial prowess.

In a video and map, the thin, sleek drone locates what appears to be a U.S. aircraft

carrier group near an island with a striking resemblance to Taiwan and sends targeting information back to shore, triggering a devastating barrage of cruise missiles toward the formation of ships.

Graphic

A look at some of China's drones

Little is known about the actual abilities of the WJ-600 drone or the more than two dozen other Chinese models that were on display at Zhuhai in November. But the speed at which they have been developed highlights how U.S. military successes with drones have changed strategic thinking worldwide and spurred a global rush for unmanned aircraft.

More than 50 countries have purchased surveillance drones, and many have started in-country development programs for armed versions because no nation is exporting weaponized drones beyond a handful of sales between the United States and its closest allies.

"This is the direction all aviation is going," said Kenneth Anderson, a professor of law at

American University who studies the legal questions surrounding the use of drones in warfare. “Everybody will wind up using this technology because it’s going to become the standard for many, many applications of what are now manned aircraft.”

Military planners worldwide see drones as relatively cheap weapons and highly effective reconnaissance tools. Hand-launched ones used by ground troops can cost in the tens of thousands of dollars. Near the top of the line, the Predator B, or MQ9-Reaper, manufactured by General Atomics Aeronautical Systems, costs about $10.5 million. By comparison, a single F-22 fighter jet costs about $150 million.

Defense spending on drones has become the most dynamic sector of the world’s aerospace industry, according to a report by the Teal Group in Fairfax. The group’s 2011 market study estimated that in the coming decade global spending on drones will double, reaching $94 billion.

But the world’s expanding drone fleets — and the push to weaponize them — have alarmed some academics and peace activists, who argue that robotic warfare raises profound questions about the rules of engagement and the protection of civilians, and could encourage conflicts.

“They could reduce the threshold for going to war,” said Noel Sharkey, a professor of artificial intelligence and robotics at the University of Sheffield in England. “One of the great inhibitors of war is the body bag count, but that is undermined by the idea of riskless war.”

**China on fast track**

# Global Race On to Match US Drone Capabilities

No country has ramped up its research in recent years faster than China. It displayed a drone model for the first time at the Zhuhai air show five years ago, but now every major manufacturer for the Chinese military has a research center devoted to drones, according to Chinese analysts.

Much of this work remains secret, but the large number of drones at recent exhibitions underlines not only China's determination to catch up in that sector — by building equivalents to the leading U.S. combat and surveillance models, the Predator and the Global Hawk — but also its desire to sell this technology abroad.

"The United States doesn't export many attack drones, so we're taking advantage of that hole in the market," said Zhang Qiaoliang, a representative of the Chengdu Aircraft Design and Research Institute, which manufactures many of the most advanced military aircraft for the People's Liberation Army. "The main reason is the amazing demand in the market for drones after 9/11."

Although surveillance drones have become widely used around the world, armed drones are more difficult to acquire.

Israel, the second-largest drone manufacturer after the United States, has flown armed models, but few details are available. India announced this year that it is developing ones that will fire missiles and fly at 30,000 feet. Russia has shown models of drones with weapons, but there is little evidence that they are operational.

Pakistan has said it plans to obtain armed drones from China, which has already sold the nation ones for surveillance. And Iran last summer unveiled a drone that Iranian President Mahmoud Ahmadinejad called the "ambassador of death" but whose

effectiveness is still unproven, according to military analysts.

The United States is not yet threatened by any of these developments. No other country can match its array of aircraft with advanced weapons and sensors, coupled with the necessary satellite and telecommunications systems to deploy drones successfully across the globe.

“We are well ahead in having established systems actively in use,” said retired Lt. Gen. David A. Deptula, the former deputy chief of staff for intelligence, surveillance and reconnaissance at the Air Force. “But the capability of other countries will do nothing but grow.”

**Raising alarm**

In recent conflicts, the United States has primarily used land-based drones, but it is developing an aircraft carrier-based version to deploy in the Pacific. Defense analysts say the new drone is partly intended to counter the long-range “carrier killer” missile that China is developing.

With the ascendance of China’s military, American allies in the Pacific increasingly see the United States as the main bulwark against rising Chinese power. And China has increasingly framed its military developments in response to U.S. capabilities.

A sea-based drone would give the United States the ability to fly three times the distance of a normal Navy fighter jet, potentially keeping a carrier group farther from China’s coast.

This possible use of U.S. drones in the Pacific has been noted with alarm in news reports in China as well as in North Korea's state-run media.

There are similar anxieties in the United States over China's accelerating drone industry. A report last November by the U.S.-China Economic and Security Review Commission noted that the Chinese military "has deployed several types of unmanned aerial vehicles for both reconnaissance and combat."

In the pipeline, the report said, China has several medium- and high-altitude long-endurance drones, which could expand China's options for long-range surveillance and attacks.

China's rapid development has pushed its neighbors into action. After a diplomatic clash with China last fall over disputed territories in the South China Sea, Japan announced that it planned to send military officials to the United States to study how it operates and maintains its Global Hawk high-altitude surveillance drones. In South Korea, lawmakers this year accused China of hacking into military computers to learn about the country's plans to acquire Global Hawk, which could peer into not only North Korea but also parts of China and other neighboring countries.

On top of the increasing anxieties of individual countries, there also are international concerns that some governments might not be able to protect these new weapons from hackers and terrorists. Sharkey, the University of Sheffield professor who also co-founded the International Committee for Robot Arms Control, noted that Iraqi insurgents, using a $30 piece of software, intercepted live feeds from U.S. drones; the video was later found on the laptop of a captured militant.

**Relaxing U.S. export controls**

But with China and other countries beginning to market their drones, the United States is looking to boost its sales by exploring ways to relax American export controls.

Vice Adm. William E. Landay III, director of the Defense Security Cooperation Agency overseeing foreign military sales, said at a Pentagon briefing recently that his agency is working on preapproved lists of countries that would qualify to purchase drones with certain capabilities. “If industry understands where they might have an opportunity to sell, and where they won’t, that’s useful for them,” Landay said.

General Atomics, the San Diego-based manufacturer of the U.S. Predator drones, has received approval to export to the Middle East and Latin America an unarmed, early-generation Predator, according to company spokeswoman Kimberly Kasitz. The company is now in talks with Saudi Arabia, the United Arab Emirates and Egypt, among others, she said.

At the same time, U.S. officials have sought to limit where others sell their drones. After Israel sold an anti-radar attack drone to China, the Pentagon temporarily shut Israel out of the F-35 Joint Strike Fighter program to register its disapproval.

In 2009, the United States also objected to an Israeli sale of sophisticated drones to Russia, according to diplomatic cables released by the anti-secrecy group WikiLeaks. A smaller co-production deal was later brokered with the Russians, who bristled when Georgia deployed Israeli surveillance drones against its forces during the 2008 war between the two countries.

But for China, there are few constraints on selling. It has begun to show its combat drone prototypes at international air shows, including last month in Paris, where a Chinese manufacturer displayed a craft, called the Wing-Loong, that looked like a Predator knockoff. Because of how tightly China controls its military technology, it is unclear how far along the Wing-Loong or any of its armed drones are from actual production and operation, defense analysts say.

According to the Aviation Industry Corp. of China, it has begun offering international customers a combat and surveillance drone comparable to the Predator called the Yilong, or "pterodactyl" in English. Zhang, of the Chengdu Aircraft Design and Research Institute, said the company anticipates sales in Pakistan, the Middle East and Africa.

However, he and others displaying drones at a recent Beijing anti-terrorism convention played down the threat of increasing Chinese drone technology.

"I don't think China's drone technology has reached the world's first-class level," said Wu Zilei, from the China Shipbuilding Industry Corp., echoing an almost constant refrain. "The reconnaissance drones are okay, but the attack drones are still years behind the United States."

But Richard Fisher, a senior fellow at the Washington-based International Assessment and Strategy Center, said such statements are routine and intended to deflect concern about the nation's expanding military ambitions.

"The Chinese are catching up quickly. This is something we know for sure," Fisher said. "We should not take comfort in some perceived lags in sensors or satellites capabilities.

Those are just a matter of time.”

# Have US Drone Wars Opened a Pandora's Box?

Have U.S. drone wars opened a Pandora's Box?

By Philip Ewing Tuesday, July 5th, 2011 12:00 pm
Posted in International

When American unmanned aircraft fly over foreign countries, attack and kill people there, that doesn't necessarily constitute "war," President Obama argues. Tom Ricks says that when U.S. drones kill bad guys in third nations, it's more akin to police work in a rough neighborhood than war. But hang on, argues Sanjeev Miglani at Reuters' Afghan Journal blog — are Americans ready to handle the blowback from carrying on a perpetual drone campaign around the world?

Writes Miglani:

*The idea that the United States can arrogate to itself the right of life and death of people around the world can set off a dangerous precedent. What happens if India decides to do a bit of police action of its own in next door Pakistan. Unlike the CIA, India has actually built up a legal case against the founder of the Lashkar-e-Taiba, Hafeez Sayeed, for involvement in the November 2008 attacks on Mumbai. Given the lack of action by Pakistani authorities, should India take the law into its hands and target Sayeed and his associates for the assault ?*

*Or as Greg Scoblete says in the Real World Compass blog, what if Iran develops the capability to fly drones of its own and blows up the suburban Virginia home of a CIA official that is suspects is instigating violence in Iran, how will America react ? Surely it is not going to say this is police action, but an act of war, or at the very least a terrorist strike on the homeland.*

*The U.S. leads the world in the use of unmanned aircraft for warfare by a distance, but it can't be very long before other nations scale up their capabilities in unmanned aerial vehicles (UAV) as they are also known.*

*The drone technology may be sophisticated, but it can be reverse-engineered and replicated (the Chinese are reportedly already doing it). Forty countries already have UAVs in their arsenals, as do reportedly non-state actors such as Hezbollah. Today the U.S. is able to fly its drones over Waziristan and Yemen, but it is not inconceivable that in the future others too might be able to fly their drones over New York and Washington.*

Not inconceivable at all, but this argument misses the point: When the U.S. conducts drone attacks, it does so with authorization from the local host government, not as an

attacking power — or so we open-source normies are told. (When we can find out anything at all.) And in the case of Libya, American Predators are part of the multi-national force that Obama spent weeks assembling, and they're following attacks by manned American warplanes. If Iran approached the U.S. government and asked for permission for UAV orbits over Washington, it would be disappointed with the response — so if it tried them, that would be an old-fashioned act of war.

The broader idea here is worth considering, and it dovetails with this summer's scuffle over the War Powers Resolution: Do presidents now have the authority, in perpetuity, to conduct low-level attacks anywhere in the world? The U.S. will never run out of enemies. When they pop up in Western countries, American officials can call allies in, say, Germany, and ask that they be arrested. But when terrorist suspects hide in lawless failed states such as Yemen and Somalia, can American presidents just order their deaths, then the deaths of the ones that come after, and so on — forever? Many Americans might say yes, that they still subscribe to President Bush's argument that we've gotta fight 'em over there so we don't have to fight 'em here. What's extraordinary is that we seem to have arrived at this point without realizing it.

Congressional lawmakers and the president apparently consider this matter settled, that Bush's drone campaign in Pakistan, which Obama has intensified, proved the point that the U.S. has to to be able to act decisively. Maybe Bush and Obama both believe they've addressed this issue when they've included vague lines in their speeches about "taking the fight to the enemy" or "doing whatever we have to do to protect America." But doesn't it seem as though this expansion in presidential power happened almost without debate? Although Congress picked a fight with the White House over Libya and the War Powers Resolution, most lawmakers have remained silent about the larger questions on America's drone wars, apparently satisfied about the president's authority to commit these attacks.

That, in turn, could be why Obama was so dismissive about congressional arguments that he has violated the War Powers Resolution. Not only has Obama been "consulting," on Libya as the law requires, he might argue, Congress years ago conceded the president's ability to conduct UAV attacks as he sees fit, which is part of what the U.S. is doing in Libya. No politician wants to be seen tying the hands of American counter-terrorism, which is why the House's actions on Libya were structured to embarrass or criticize the president, but not actually affect the U.S. campaigns already underway — and no one mentioned Yemen or Somalia.

So as for Miglani's fear "that the United States can arrogate to itself the right of life and death of people around the world?" That, for America's top leadership, apparently is a done deal.

# 'Hands-free' Landing Is a Step Toward Unmanned Naval Flight

**'Hands-free' landing is a step toward unmanned naval flight**

An F/A-18D Hornet lands aboard the aircraft carrier Dwight D. Eisenhower, the first arrested landing of a surrogate aircraft emulating an unmanned vehicle. (U.S. Navy)

By Bill Sizemore
The Virginian-Pilot
© July 8, 2011

Are the days of "Top Gun" coming to an end?

Not yet. But the Navy moved a step closer to a new era of unmanned carrier-based aerial combat last weekend.

Aboard the Norfolk-based aircraft carrier Dwight D. Eisenhower off the Virginia coast Saturday, an F/A-18D Hornet, modified to emulate an unmanned aircraft, made its first carrier touchdown without a pilot's guiding hands.

A pilot and a flight officer were in the cockpit in case human intervention was needed, but the landing was "hands-free" - controlled by a linked computer network on the ship and the plane.

The F/A-18D fighter jet was a stand-in for the X-47B, a bat-winged, fighter-sized unmanned aircraft under development by Northrop Grumman Corp. as part of the Navy's Unmanned Combat Air System Demonstration program.

The pilot of the surrogate plane, Lt. Jeremy DeBons, said the hands-free landing was

in one sense an incremental step, because fighter jets are already capable of being coupled with a carrier's computer system for assistance in touchdowns.

Still, DeBons said, because this is a new system, extra vigilance was in order.

"As any test pilot will tell you, we're always on guard," he said. "It's not only hands-free. It's hands very close to the controls if we have to take over."

The successful automated landing on the Eisenhower was "a very significant step" toward eventual use of unmanned drones on carriers, Rear Adm. Bill Shannon, the program executive officer, said in a conference call with reporters Thursday.

That doesn't mean the end of manned naval flight is anywhere on the horizon, said Capt. Jaime Engdahl, the program manager.

"That is not the goal," Engdahl said. "The Navy's goal is to seamlessly integrate unmanned systems into the fleet. It's really in the gaps - where it can complement manned assets and expand the Navy's capability in intelligence collection, surveillance and reconnaissance."

For instance, he said, one of the gaps the Navy hopes to fill with drones is in long-duration flights that are beyond the capacity of a human crew.

Still, there is little doubt that Navy drones eventually will move beyond a surveillance role, said Peter Singer, a senior fellow at the Brookings Institution, a Washington think tank, who has written a book on automated warfare.

The Air Force's Predator drones were originally designed for surveillance, he noted, but are now widely used for dropping bombs. There is no reason Navy drones couldn't be used the same way or even for air-to-air combat, he said.

Human pilots aren't going away anytime soon, but the dawn of unmanned naval flight portends a changing role for them, Singer said.

"We previously judged the value of the aviator by technical skill - particularly at carrier deck landings," he said. "I think increasingly we're going to judge the human aviator not so much on quick reactions in their fingertips but on that mushy gray thing in their

skull and that pulsating thing in their chest.

"We're going to judge them less on things like carrier deck landings and more on things like when is it proper to shoot or not - a sense of strategy, a sense of right and wrong, a sense of awareness."

There's also little doubt that the changes will come sooner rather than later, Singer said. He used a historical anecdote to illustrate the point.

On Oct. 9, 1903, The New York Times predicted that flying machines would take "one to ten million years" to develop. That same day, the Wright brothers began assembling their first airplane. Seven years later, Eugene Ely flew off a wooden platform built on the bow of the cruiser Birmingham in Hampton Roads, and the era of naval aviation was born.

Modifications to accommodate the unmanned system on the Eisenhower began last fall. Initial surrogate testing, which proved the system was ready, took place during the ship's sea trials the week of June 13.

Flight testing of the X-47B unmanned aircraft is under way at Edwards Air Force Base, Calif., and will move to Patuxent River Naval Air Station in Maryland later this year.

The Navy is aiming to land the X-47B on a carrier in 2013.

JULY 2, 2011

A Roboticist's Trip From Mines to the Moon

By JAMES R. HAGERTY

Robots created by William "Red" Whittaker have crawled into mines and volcanoes, crossed deserts, won a 60-mile road race, helped clean up nuclear waste and harvested alfalfa. He has sheaves of academic awards and more than a dozen U.S. patents. "I have a very robot-centric view of the universe," he said.

Carnegie Mellon robotics professor William "Red" Whittaker wants to send a robot to the moon. (Video Courtesy of Astrobotic Technology and Carnegie Mellon University)

Now the 63-year-old professor of robotics at Pittsburgh's Carnegie Mellon University is gambling on his boldest venture yet: designing and making a spacecraft capable of carrying one of his robots to the moon.

Mr. Whittaker and a band of students are among 29 teams vying for the Google Lunar X Prize, which will award $20 million to the first privately funded team whose robot reaches the moon, travels 500 meters and flashes data back to the Earth. Though no one on his team has ever made a spacecraft, Mr. Whittaker is undaunted by his goal of reaching the moon in April 2014.

# A Roboticist's Trip From Mines to the Moon

Loping around a white-walled university workshop, the brawny, 6-foot-3-inch-tall professor shows off shiny aluminum parts for the landing craft, spread around the floor like giant Lego pieces. "Like most things in life," he said, "it comes without instructions."

Ryan Donnell for The Wall Street Journal.

Williams 'Red' Whittaker with his lunar lander at the Robotics Institute at Carnegie Mellon University.

Mr. Whittaker's original plan was to make only the lunar robot (or "rover") and entrust the design and building of the landing craft to aerospace experts. But he grew impatient waiting for their plans and decided two years ago to try his hand at spacecraft. Mr. Whittaker, who sometimes refers to himself in the third person as if narrating a tale of adventure, recalls thinking, "Now Red's making a lander."

He is bored by incremental research. He likes projects that "border on the unachievable."

What makes Mr. Whittaker shoot for the moon may be the same taste for risk that impelled him as a teenager to try wrestling an ape at a carnival—the ape won—and dabble in boxing. He credits his parents for encouraging exploration and boldness. His father, a World War II Air Force bombardier, sold explosives used in mining and road construction. His mother was a science teacher who also flew planes. Once she flew him under a bridge. While figuring out what to do with his life, he spent two years in the Marines, rising to the rank of sergeant. Then, after earning a civil engineering degree at Princeton University in 1973, Mr. Whittaker moved to Carnegie Mellon for graduate

school.

**Photos: Fly Me To the Moon**

Astrobotic Technology

View the process of building the model lunar lander at Carnegie Mellon.

Two decades ago, he bought a hillside cattle ranch 90 miles east of Pittsburgh after concluding that his academic life was too sedentary and citified. He wanted physical activity "that also adds up to something" and "to do it with my muscles, not my money." He also likes tinkering with old machinery; he recently rebuilt an old pickup truck.

Mr. Whittaker came up with some of the earliest techniques using global-positioning systems to create farm and mining equipment that steers itself. Early systems weren't fast enough to calculate where a moving vehicle was, so he needed to "create a computer model to estimate where you are while predicting and controlling where you are going."

"A lot of times you don't really have to be good, just first," Mr. Whittaker said. He believes in getting the idea "90% right" and plunging into production by trial and error, rather than seeking the perfect design.

Mr. Whittaker's right-hand man on the lander design is Jason Calaiaro, 24, a mechanical engineer who plays the drums and was thinking about going to cooking school before getting the space gig. Mr. Whittaker tends to attract like-minded colleagues, and Mr. Calaiaro shares Mr. Whittaker's supreme self-confidence. "We are

very capable people who have no problem putting in 90-hour weeks," he said.

**Spare Parts**

Before settling on robotics, William "Red" Whittaker briefly considered computer science but decided that field was too well-established. "Computing," he says, "was going to have a good future with or without me."

Mr. Whittaker's first robotic triumph was in swiftly designing and deploying robots on wheels that inspected damage and cleaned up waste at the Three Mile Island nuclear plant in the early 1980s.

He recently drew inspiration from an essay by Orville Wright titled "How We Made the First Flight." He was struck by how the Wright Brothers "transformed the world's view of flying from impossibility to fact."

A part-time rancher, Mr. Whittaker says, "I'm very untraditional in the way I knock my hay down." He often mows it in the dark or in the rain. That way, he says, the grass has more time to dry in the sun after the mowing.

Lee Gutkind, who wrote "Almost Human," a book about Mr. Whittaker and other robot designers at Carnegie Mellon, says the engineering "gearheads" like Mr. Whittaker have always tended to be louder and more physical than the computer software "code monkeys" who work with them.

Their first concept involved a traditional three-stage system, in which the first two stages fall off after spending their fuel. But that would have been expensive and complicated. Mr. Whittaker decided to create a single-stage lander, which he saw as less fuel-efficient but more likely to get the job done.

Excess weight is a bad idea. When possible, he avoids moving parts: The four legs that are to touch down on the moon have no joints and won't need to be repositioned for landing. He is skimping on shock absorbers. "I will be betting on a great landing," guided by sensors, Mr. Whittaker said. The lander is "squat and wide," to reduce risks of tipping over on the moon or "flexing" during takeoff from Earth.

The design may look inelegant, said Mr. Whittaker, but he recalls the story of Dick Fosbury, whose highly unorthodox method of high jumping—the Fosbury flop—at first drew laughter and then won him a gold medal at the Olympic Games in 1968.

Some of his robots haven't worked out. One trundled into a coal mine and couldn't get

out; a Hummer programmed to drive itself flipped over. It is counterproductive to dwell on the risks, he said: "Worry is a formula for failure."

Design breakthroughs don't come while taking a shower or "thinking about the top 20 pop songs," he said. Instead, they come from focusing intensely on a goal, or "dwelling in the intention," as he put it. Creativity, he said, happens "in the heat of the action" rather than while musing in a comfortable perch.

Mission statements should be brief: "Strip away all of the 'how' and the tangential," he advised. Albert Einstein's goal might have been boiled down to "understand the universe," says Mr. Whittaker. His own goal is more modest: "land on the moon."

## NASA IG warns of possible weather satellite coverage gap

July 6, 2011 — 6:19pm ET | By David Perera

Artist's rendering of the NPP satellite.
Image: NOAA

A satellite meant to fill in a potential gap in satellite weather coverage runs the risk of running twice late, warns a NASA inspector general report.

The report, dated June 2, says the NPOESS Preparatory Project satellite is scheduled for an October 2011 launch but that potential ground system integration and testing issues might require a delay.

NPP, a minibus-sized satellite that was first meant to act as earth observation coverage gap filler in-anticipation of the now-dissolved National Polar-orbiting Operational Environmental Satellite System program, was supposed to have launched in October 2006 at a lifecycle cost of $560 million.

Current estimates peg the lifecycle cost at $864 million, although the report lays the blame for the delay and cost increase squarely outside of NASA, on the NPOESS Integrated Program Office, which was staffed by Defense Department, NASA and National Oceanic and Atmospheric Administration personnel.

NPOESS, plagued by cost overruns, was dissolved by the White House in February 2010 into two separate projects, one led by NASA and NOAA, the other by the DoD. As part of that disbanding, contracts for associated ground systems went away from the Air Force and to NASA and NOAA, leading to delivery delays, the report says. It wasn't until November 2010 that the ground system hardware and contracts were finally

transferred, the report adds.

NPP program management told auditors that it typically takes 15 months to perform ground system integration and testing after integration of the last instrument, which for NPP occurred in June 2010. While that theoretically makes an October 2011 NPP launch possible, auditors doubt its plausibility, since NPP staff also said they expect some integration issues could take longer than 15 months.

Were a delay to occur, the next window for launch would be in February 2012, which would add $35 million to the price tag and could result in a gap in data continuity, auditors say.

A NASA spokeswoman did not immediately return a call inquiring about the possibility of a delay.

For more:
- download the report, IG-11-018 (.pdf)

# This 45-Mile "Wi-Fi" Could Connect a Smarter Power Grid

Tuesday, June 28, 2011

**This 45-Mile "Wi-Fi" Could Connect a Smarter Power Grid**
A startup's wireless technology sends low-bandwidth signals over long distances, even underground.

By Tom Simonite

If your home Wi-Fi router wasn't cooped up indoors, it could send a signal about a 20th of a mile before the signal became too weak and distorted for a computer to receive it. Technology developed by San Diego startup On-Ramp Wireless uses the same frequency, but less power, to send data signals 45 miles, thanks to algorithms that make the signals very resistant to noise.

The technology, called Ultra-Link Processing, transfers data at a very low rate compared with a home broadband connection. But On-Ramp intends to offer it as a way to enable "smart energy" grids, in which simple sensors installed in home energy meters, for example, report local activity back to utilities, allowing them to manage power generation and distribution more intelligently.

Smart-grid infrastructure is needed to cope with the fluctuating output of renewable energy sources at large scale, and it could make feasible micro-generation, whereby consumers make their own power and sell any surplus back to the grid. Today's smart-grid sensors typically use Wi-Fi-like technology with Wi-Fi-like ranges, or unlicensed radio bands that can reach a couple of miles. Cellular networks can also be used, but these connections are under growing pressure from data-hungry phones and tablets.

"There's no technology available for devices that just need a trickle of connectivity over long distance," says On-Ramp's chief technology officer, Ted Myers, who says that with a clear line of sight, On-Ramp's technology can send a signal 45 miles. He is targeting devices that use less than 50 bits per second, roughly 100,000 times less than the average U.S. broadband speed of five megabits per second.

A trial network in San Diego requires just 35 strategically located access points to collect data from smart meters and other devices equipped with On-Ramp's technology across a 4,000-square-mile area. "It boils down to a cost advantage," says Myers. "You need fewer access points this way." California utility PG&E is currently rolling out smart meters based on more established technology which will require over

1,000 access points to cover the same area, Myers claims.

With the aid of a $2.1 million grant from the Department of Energy, On-Ramp is now working with utility San Diego Gas and Electric to monitor hard-to-reach pieces of energy infrastructure. In other trials, On-Ramp is working with oil company Shell to link up pressure sensors on gas pipelines in Europe, and with defense contractors interested in tracking objects equipped with Ultra-Link Processing transmitters.

At the heart of the technology is a suite of proprietary algorithms for transmitting and decoding data signals. These enable On-Ramp's receivers to pluck a signal that has been weakened by distance out of the noise generated by other Wi-Fi and radio signals in the same frequency bands. The technology can even pick up signals that are weaker than the surrounding background noise, says Myers—something that devices using cellular or mesh networks cannot do. According to standard models for predicting wireless performance in real-world scenarios, On-Ramp's technology is able to use signals 20 percent weaker than those needed for a cellular link, and 35 percent weaker than those needed for grid sensors that link together into a mesh network, he says. It can even send signals from sensors underground, for example on subterranean electric or gas lines.

Chips that have On-Ramp's proprietary technology built in are required, though. Devices used in trial deployments so far have been based on a first-generation chip produced in Taiwan. A version due this fall, the MicroNode pictured, is roughly a third cheaper, and it will make smart meters equipped with On-Ramp's technology competitive with those already being rolled out by some utilities, says Myers.

Rajit Gadh, who researches smart-grid technology and deployments at the University of California, Los Angeles, says that utilities are certainly interested in reducing the cost of smart-grid infrastructure, and adds that new types of wireless networks could help. "There's not an exact match between the technology that's out there and what the smart grid needs to really deliver," says Gadh. "There will be wireless links operating at a range of different frequencies used in different scenarios, for example urban or rural areas, or developing-world cities that are denser."

Most technology in use today, Gadh says, was developed for other purposes. For example, many smart-grid deployments use the Zigbee protocol that was originally intended for linking up appliances in networked homes. However, On-Ramp is competing with many other companies bidding to connect the parts of the smart grid, Gadh points out, and most of these use more established technologies that utilities are

much more familiar with.

Copyright Technology Review 2011.

**Real U.S. Stealth-Tech Advantage: Its Assembly Lines**

- By David Axe July 6, 2011 | 7:00 am | Categories: Air Force
  **@daxe** · 709 followers

For more than 20 years, the U.S. Air Force had a world monopoly on radar-evading technology — and with it, a huge advantage over any rival. Several generations of stealth fighters and bombers, from the earliest F-117s to the 1990s-vintage B-2s and today's F-22s, have helped win wars, take down regimes and exert U.S. influence across the globe.

Then something happened. In an eventful two years, the United States has apparently lost its stealth monopoly to Russia, China and several other countries that have already flown their own stealth-fighter prototypes — or might soon. U.S. stealth planes are still better and far more numerous than any other country's, and will be for a long time. But they're no longer alone.

The implications could be enormous, for the United States and the world.

Or not. There's evidence that most countries are merely bluffing with their stealth-fighter plans. In that case, U.S. stealth dominance could continue … only slightly diminished.

# Real US Stealth-Tech Advantage: Its Assembly Lines

The first challenger to U.S. radar-evading warplanes was the Russian T-50, debuting in January 2010. The Chinese J-20, pictured, followed 11 months later. Spurred on by the T-50 and J-20, several Asian nations announced their own stealth-fighter schemes. India signed on for a version of the T-50. Japan and South Korea began designing stealth warplanes of their own.

The stealth race shows no outward sign of slowing. Rumors abound of a *second* Chinese stealth jet that could begin testing any day now.

But it's not clear how many of these new stealth fighters will ever enter full-rate production. Indeed, it's possible some are not even meant for front-line service.

That's the hidden irony of the stealth arms race. While it might appear that the United States has lost its lead in the design and manufacture of "invisible" warplanes, the escalating global demand for stealth could end up working in the United States' favor, by creating a market for the latest fighters that didn't exist before — and one only the United States can really afford to exploit.

The key is *scale*.

It's one thing to design a viable stealth plane, and even to show off a prototype or two. It's entirely another thing to mass-produce combat-ready stealth fighters at a price the world's air forces can afford. "Talk is cheap," my old boss (and Danger Room co-founder) Sharon Weinberger used to say. "Military aircraft are expensive."

It's possible only the United States has the industrial capacity and domestic market sufficient to make its stealth planes economical on the *world* market. That's the whole rationale behind the Lockheed Martin F-35 Joint Strike Fighter, the fourth (but not last)

U.S. stealth warplane.

The U.S. Air Force, Navy and Marines could buy as many as 3,000 F-35s over the next 30 years. No other country even possesses that many fighters, much less plans to replace them all with stealth models. “It [the F-35] is a versatile aircraft, less than half the total cost of the F-22, and can be produced in quantity with all the advantages produced by economies of scale,” former Secretary of Defense Robert Gates said two years ago.

Gates was on to something (even if the JSF turned out to be not as cheap as he hoped). With development costs mostly paid for by Washington, and Lockheed’s investment protected by the promise of huge domestic orders, the F-35 is positioned to be the United States’ — and the world’s — first relatively affordable, exportable stealth fighter. A number of countries have already placed orders, and more should follow.

Some might question whether a plane priced at $100 million per copy *before* development and support expenses is truly economical. And they’re right to be skeptical. But China’s J-20 could end up costing even more than the F-35, *if* it enters full-scale production at all. Japan pays more than $100 million for each of its current, non-radar-evading F-2 warplanes — and would probably have to shell out double that per copy for its planned “ATD-X” stealth fighter.

Foreign governments are aware of the high cost of developing and buying homemade stealth fighters. And that’s why most of them probably don’t intend on following through with indigenous warplane programs. Instead, many countries are working on stealth technology as a political bargaining chip, and as practice for their aerospace industries. Their goal is to team up with other countries on stealth.

Take Japan, for example. No one seriously believes Tokyo is prepared to devote a full 5 percent of its annual defense budget to purchase a handful of homemade ATD-X

stealth fighters. The Pentagon will probably end up spending just 3 percent of its budget for a proportionally much larger fleet of F-35s. Producing its own stealth fighters could bankrupt the Japanese military.

More likely, the Japanese government is budgeting a few hundred million dollars to refining basic stealth technology, with the real goal of proving to Lockheed that Japanese industry deserves to participate in the production of F-35s, if and when Tokyo formally decides to acquire the type. Same goes for South Korea, which could also acquire the F-35 and hopes to make parts for the jet. It's worth keeping an eye on where these countries' stealth components wind up. But neither Japan nor South Korea is about to build a fleet of rivals to stealthy U.S. warbirds.

Russia, for its part, may also be more of a maker of stealth parts than a stealth jets. Moscow perhaps always intended India to help pay for the stealth T-50 fighter's development, as Russia probably couldn't afford the T-50 all on its own.

That leaves China. While there is speculation that Beijing might try to sell radar-evading fighters to Pakistan, so far China is going it alone on stealth. Whether the Chinese can afford large numbers of stealth planes remains to be seen. Double-digit GDP growth can't last forever.

Once the dilettantes are factored out, there are really only three countries making viable stealth fighters, and only two — the United States and China — capable of making them on their own. If there exists a market for 4,000 stealth warplanes over the next three decades, probably 3,500 will be U.S. models.

That's not a monopoly, but it's pretty close. The U.S. radar-evading advantage might not be as overwhelming as it once was, but it could still endure for decades — thanks mostly to the incredibly high cost of stealth.

# Real US Stealth-Tech Advantage: Its Assembly Lines

*Photo: Chinese Internet*

# Moore's Law Meets Exascale Computing

June 29, 2011

Moore's Law Meets Exascale Computing
Michael Feldman

There are no exascale supercomputers yet, but there are plenty of research papers on the subject. The latest is a short but intense white paper centering on some of the specific challenges related to CMOS technology over the next decade and a half. The paper's principal focus is about dealing with the end of Moore's Law, which, according to best predictions, will occur during the decade of exascale computing.

Titled Exascale Research: Preparing for the Post-Moore Era (PDF), the paper is authored by HPC experts Marc Snir, Bill Gropp and Peter Kogge, who argue that we need to start using CMOS technology much more efficiently, while simultaneously accelerating the development of its replacement.

One of the tenets of supercomputing, and information technology in general, is that processors are expected to get more powerful and less expensive each year. Like the shark that needs to keep swimming to stay alive, the IT industry is based on the assumption that the hardware has to keep moving forward to support the expectations of the market.

This is certainly true for exascale proponents, who see the next level of HPC capability as a way to move forward on big science problems and help solve global challenges like climate change mitigation and the development of alternative energy sources. In the US, there is also the need to support our nuclear stockpile with compute-intensive virtual simulations -- a task that is becoming increasingly difficult as the original expertise in designing and testing nuclear weapons disappears.

National security, too, has become very dependent on supercomputing. As the

authors state, "In
an era where information becomes the main weapon of war, the US cannot afford to be outcomputed anymore that it can afford to be outgunned."

It's a given that the semiconductors behind exascale computing will, at least initially, use CMOS, a technology that's been in common use since the 1970s. The problem is that CMOS (complementary-symmetry metal–oxide–semiconductor) is slowly giving way to the unrelenting laws of physics. Due to increasing leakage current, voltage scaling has already plateaued. That occurred nearly a decade ago when transistor feature size reached 130 nm. The result was that processor speeds leveled off.

And soon feature scaling will end as well. According to the white paper, CMOS technology will grind to a halt sometime in the middle of the next decade when the size of transistors reaches around 7 nm -- about 30 atoms of silicon crystal. As the authors put it:

We have become accustomed to the relentless improvement in the density of silicon chips, leading to a doubling of the number of transistors per chip every 18 months, as predicted by “Moore’s Law”. In the process, we have forgotten “Stein’s Law”: "If something cannot go on forever, it will stop."

And unfortunately there is currently no technology to take the place of CMOS, although a number of candidates are on the table. Spintronics, nanowires, nanotubes, graphene, and other more exotic technologies are all being tested in the research labs, but none are ready to provide a wholesale replacement of CMOS. To that end, one of the principal recommendations of the authors is for more government funding to accelerate the evaluation, research and development of these technologies, as a precursor to commercial production 10 to 15 years down the road.

It should be noted, as the authors do, that the peak performance of

supercomputer has increased faster than CMOS scaling, so merely switching technologies is not a panacea for high performance computing. In particular, HPC systems have gotten more powerful by increasing the number of processors, on top of gains realized by shrinking CMOS geometries. That has repercussions in the failure rate of the system, which is growing in concert with system size.

The larger point is that the end of CMOS scaling can't be compensated for just by adding more chips. In fact, it's already assumed that the processor count, memory capacity, and other components will have to grow substantially to reach exascale levels, and the increased failure rates will have to be dealt with separately.

On the CMOS front, the main issue is power consumption, most of which is not strictly related to computation. The paper cites a recent report that projected a 2018-era processor will use 475 picojoules/flop for memory access versus 10 picojoules/flop for the floating point unit. The memory access includes both on-chip communication associated with cache access and off-chip communication to main memory.

To mitigate this, the authors say that smarter use of processor circuitry needs to be pursued. That includes both hardware (e.g., lower power circuits and denser packaging) and software (e.g., algorithms than minimize data movement and languages able to specify locality). More energy-aware communication protocols are also needed.

The good news is that most of the performance/power improvements discussed in the paper will also benefit the commodity computing space. But the authors also say that some of the technology required to support future HPC systems will not be needed by the volume market:

We need to identify where commodity technologies are most likely to diverge

from the technologies needed to continue the fast progress in the performance of high-end platforms; and we need government funding in order to accelerate the research and development of those technologies that are essential for high-end computing but are unlikely to have broad markets.

The authors aren't suggesting we need to build graphene supercomputers, while the rest of the world moves to spintronics. But there may be certain key technologies that can be wrapped around post-CMOS computing that will be unique to exascale computing. As always, the tricky part will be to find the right mix of commodity and HPC-specific technologies to keep the industry moving forward.

# IBM Announces Computer Memory Breakthrough

IBM announces computer memory breakthrough

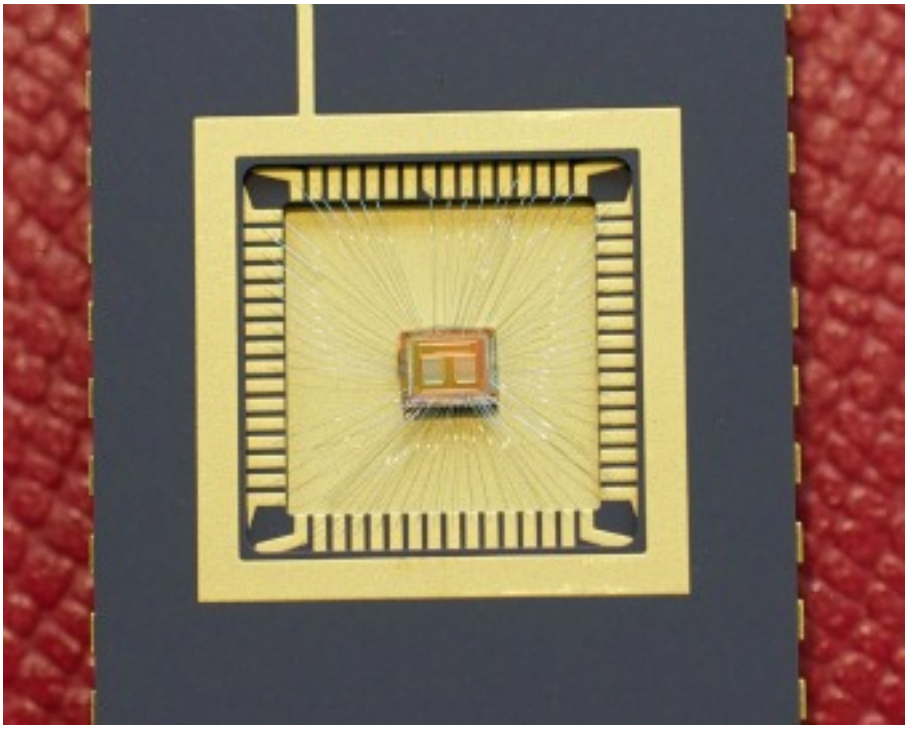
Phase-change memory offers 100 times the write performance of NAND flash
**Lucas Mearian**

**June 30, 2011** (Computerworld)

IBM Thursday announced a breakthrough in computer memory technology, which may lead to the development of solid-state chips that can store as much data as NAND flash technology but with 100 times the performance and vastly greater lifespan.

Currently, NAND flash memory products, such as SSDs, have write rates as high as 2Gbit/sec.

IBM said it has produced phase-change memory (PCM) chips that can store two bits of data per cell without data corruption problems, something that has plagued PCM development from the start.



IBM's phase-change memory chip uses circuitry that is 90 nanometers in width

Like NAND flash memory, which is used in solid state drives (SSDs) and is embedded in computers like Apple's MacBook Air, PCM is nonvolatile -- meaning it retains data after its power supply is shut down.

Unlike NAND flash, PCM memory does not require that existing data be marked for deletion prior to new data being written to it -- a process known to as an erase-write cycle. Erase-write cycles slow NAND flash performance and, over time, wear it out, giving it a lifespan that ranges from 5,000 to 10,000 write cycles in consumer products and up to 100,000 cycles in enterprise-class products.

PCM can sustain up to 5 million write cycles, according to IBM.

"If you can write to flash 3,000 times, that will outlive most cell phones and MP3 players, but that's certainly not good enough for the enterprise that does that in an hour," said Christopher Sciacca, manager of communications for IBM Research in Zurich.

As organizations and consumers increasingly embrace cloud-computing models and services, ever more powerful and efficient, yet affordable storage technologies are needed, according to Haris Pozidis, manager of memory and probe technologies at IBM Research.

Pozidis said that for the past five months, teams of IBM scientists have been testing a multi-level cell (MLC) chip that's capable of storing two and eventually three bits of data, indicating that it can achieve a level of reliability that is suitable for practical applications.

Besides applications for enterprises and in the cloud, PCM may also serve as an extension for DRAM.

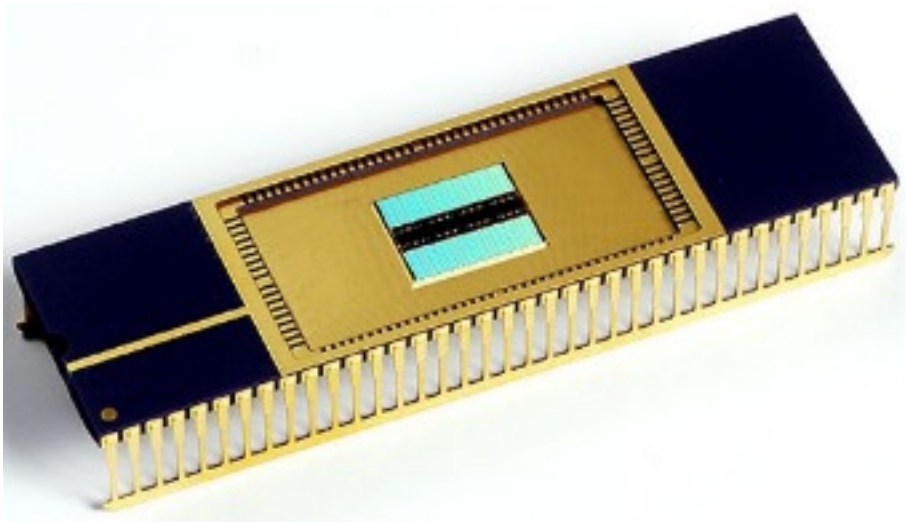
While DRAM will continue to be used as the closest memory device to the CPU for the most active data, Pozidis said, PCM, with its greater capacity, can be used for less frequently accessed data. "The PCM, which is much larger, acts as a repositor. If the data becomes hot again it will move back to the DRAM," he said.

In another scenario, Pozidis said, the CPU can talk directly to the PCM, but it thinks its talking to the DRAM using a controller. "Again, the hot data speaks to DRAM and not so hot data speaks to the PCM," he said.

DRAM is also expected to hit a technical wall in several years when it reaches lithography sizes of between 20-30 nanometers. One nanometer is roughly the size of four gold atoms.

A nascent technology, PCM is used today as a replacement for NOR, EEPROM, NVRAM memory that are currently manufactured by Micron Technology, Samsung, and South Korea's Hynix Semiconductor.

Current technology is single-level cell (SLC) PCM, which only stores one bit per cell with limited capacity. For example, Samsung produces a 512Mbit PCM chip for its GT-E2550 GSM mobile phone. Micron's Numonyx division makes a 128 Mbit PCM chip and is shipping product to several customers who use it in networking equipment, medical monitoring devices, and security cameras.



Samsung's PCM RAM chip

PCM uses electrical charges to change areas on a glassy material from crystalline to random or amorphous. The technique uses far less power than NAND flash to store data and it has data write rates up to 100 times faster because it does not first require existing data to be marked for deletion.

PCM leverages the resistance change that occurs in the material -- an alloy of various elements -- when it changes its phase from crystalline - featuring low resistance - to amorphous - featuring high resistance - to store data bits. In a PCM cell, where a phase-change material is deposited between a top and a bottom electrode, phase change can controllably be induced by applying voltage or current pulses of different strengths. These heat up the material, and when distinct temperature thresholds are reached cause the material to change from crystalline to amorphous or vice versa.

IBM scientists said they were able to solve the bit error problem associated with MLC PCM memory by using an advanced modulation coding technique, which addresses the problem of short-term drift. Short-term drift is analogous to a problem in NAND flash memory where electrons leak through the thin walls of cells and create data read errors.

In NAND flash, the problem is addressed through the use of error correction code (ECC) in controller chips. But in PCM, data errors are not corrected but avoided through the use of specialized code.

"With modulation codes you try to avoid the most probable errors. Modulation codes appear today in hard disk drives as well as optical drives such as Blu-ray discs," Pozidis said. "We apply a voltage pulse based on the deviation from the desired level and then measure the resistance. If the desired level of resistance is not achieved, we apply another voltage pulse and measure again - until we achieve the exact level."

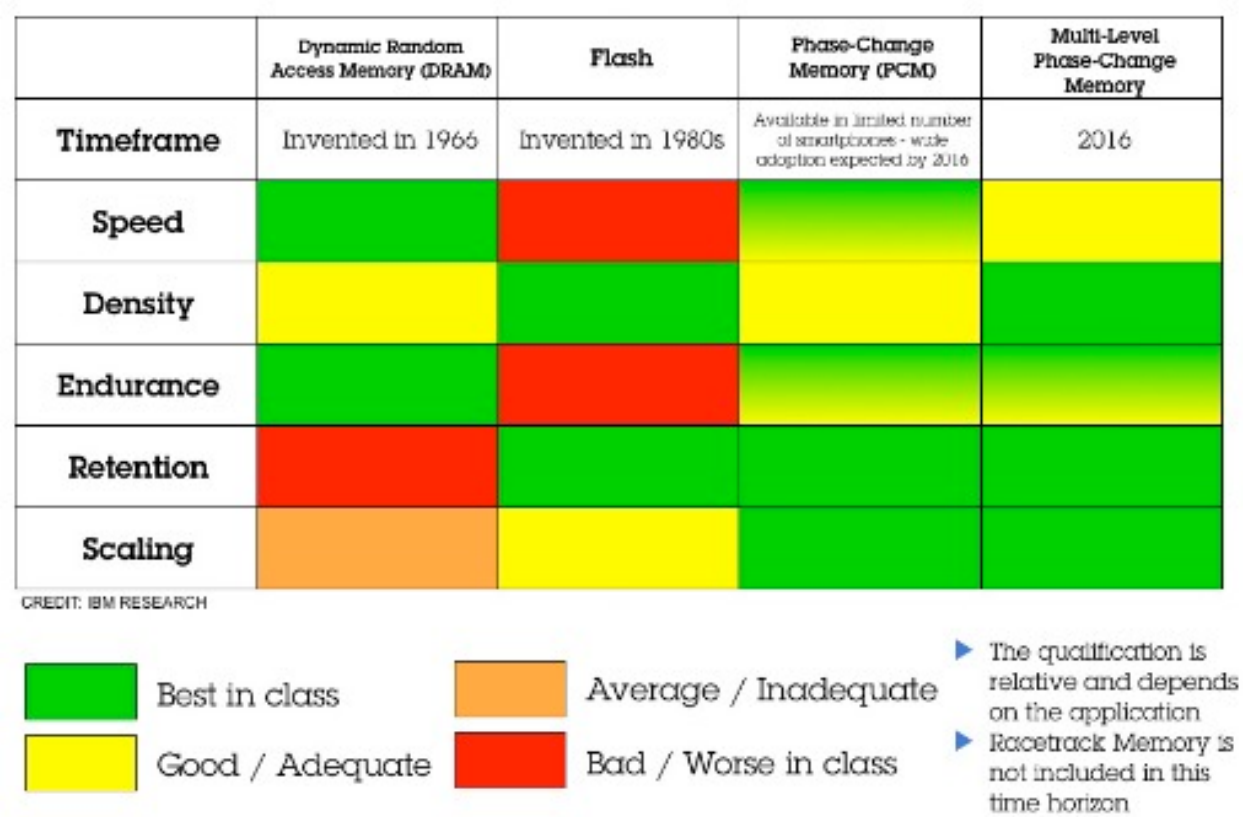
IBM scientists achieved a worst-case write latency of about 10 microseconds, which represents a 100x performance increase over even the most advanced flash memory on the market today.

Pozidis said IBM is currently using PCM circuitry that is 90 nanometers in size, or

about twice the width of today's densest SLC PCM products. But that too will shrink over time.

IBM is not planning to produce consumer grade products out of PCM, Pozidis said. The main target for the technology is to license it to memory manufacturers, such as Toshiba and Samsung, and help them accelerate the production of the memory chips for enterprise applications.

Other researchers have been combining carbon nanotube technology with PCM to create chips that sip electricity and could extend the battery life of mobile devices to weeks.




A comparison between DRAM, NAND flash, single-level PCM and multi-level PCM

## Making Speedy Memory Chips Reliable

*IBM believes a new way of encoding the bits in phase-change memory will make it reliable enough for use in servers.*

- THURSDAY, JUNE 30, 2011
- BY KATHERINE BOURZAC

IBM researchers have developed a programming trick that makes it possible to more reliably store large amounts of data using a promising new technology called phase-change memory. The company hopes to start integrating this storage technology into commercial products, such as servers that process data for the cloud, in about five years.

Like flash memory, commonly found in cell phones, phase-change memory is nonvolatile. That means it doesn't require any power to store the data. And it can be accessed rapidly for fast boot-ups in computers and more efficient operation in general. Phase-change memory has a speed advantage over flash, and Micron and Samsung are about to bring out products that will compete with flash in some mobile applications.

These initial products will use memory cells that store one bit each. But for phase-change memory to be cost-competitive for broader applications, it will need to achieve higher density, storing multiple bits per cell. Greater density is necessary for IBM to achieve its goal of developing phase-change memory for high-performance systems such as servers that process and store Internet data much faster.

The IBM work announced today offers a solution. In the past, researchers haven't been able to make a device that uses multiple bits per cell that works reliably over months and years. That's because of the properties of the phase-change materials used to store the data. Scientists at IBM Research in Zurich have developed a software trick

that allows them to compensate for this.

Advertisement

Each cell in these data-storage arrays is made up of a small spot of phase-change materials sandwiched between two electrodes. By applying a voltage across the electrodes, the material can be switched to any number of states along a continuum from totally unstructured to highly crystalline. The memory is read out by using another electrical pulse to measure the resistance of the material, which is much lower in the crystalline state.

To make multibit memory cells, the IBM group picked four different levels of electrical resistance. The trouble is that over time, the electrons in the phase-change cells tend to drift around, and the resistance changes, corrupting the data. The IBM group has shown that they can encode the data in such a way that when it's read out, they can correct for drift-based errors and get the right data.

The IBM group has shown that error-correcting code can be used to reliably read out data from a 200,000-cell phase-change memory array after a period of six months. "That's not gigabits, like flash, but it's impressive," says Eric Pop, professor of electrical engineering and computer sciences at the University of Illinois at Urbana-Champaign. "They're using a clever encoding scheme that seems to prolong the life and reliability of phase-change memory."

For commercial products, that reliability timescale needs to come up to 10 years, says Victor Zhirnov, director of special projects at the Semiconductor Research Corporation. IBM says it can get there. "Electrical drift in these materials is mostly problematic in the first microseconds and minutes after programming," says Harris Pozidis, manager of memory and probe technologies at IBM Research in Zurich. The problem of drift can be statistically accounted for in the IBM coding scheme over whatever timeframe is

necessary, says Pozidis, because it occurs at a known rate.

But phase-change memory won't be broadly adapted until power consumption can be checked, says Zhirnov. It still takes much too much energy to flip the bits in these arrays. That's due to the way the electrodes are designed, and many researchers are working on the problem. This spring, Pop's group at the University of Illinois demonstrated storage arrays that use carbon nanotubes to encode phase-change memory cells with 100 times less power.

# Graphene Enables Invisibility Cloak

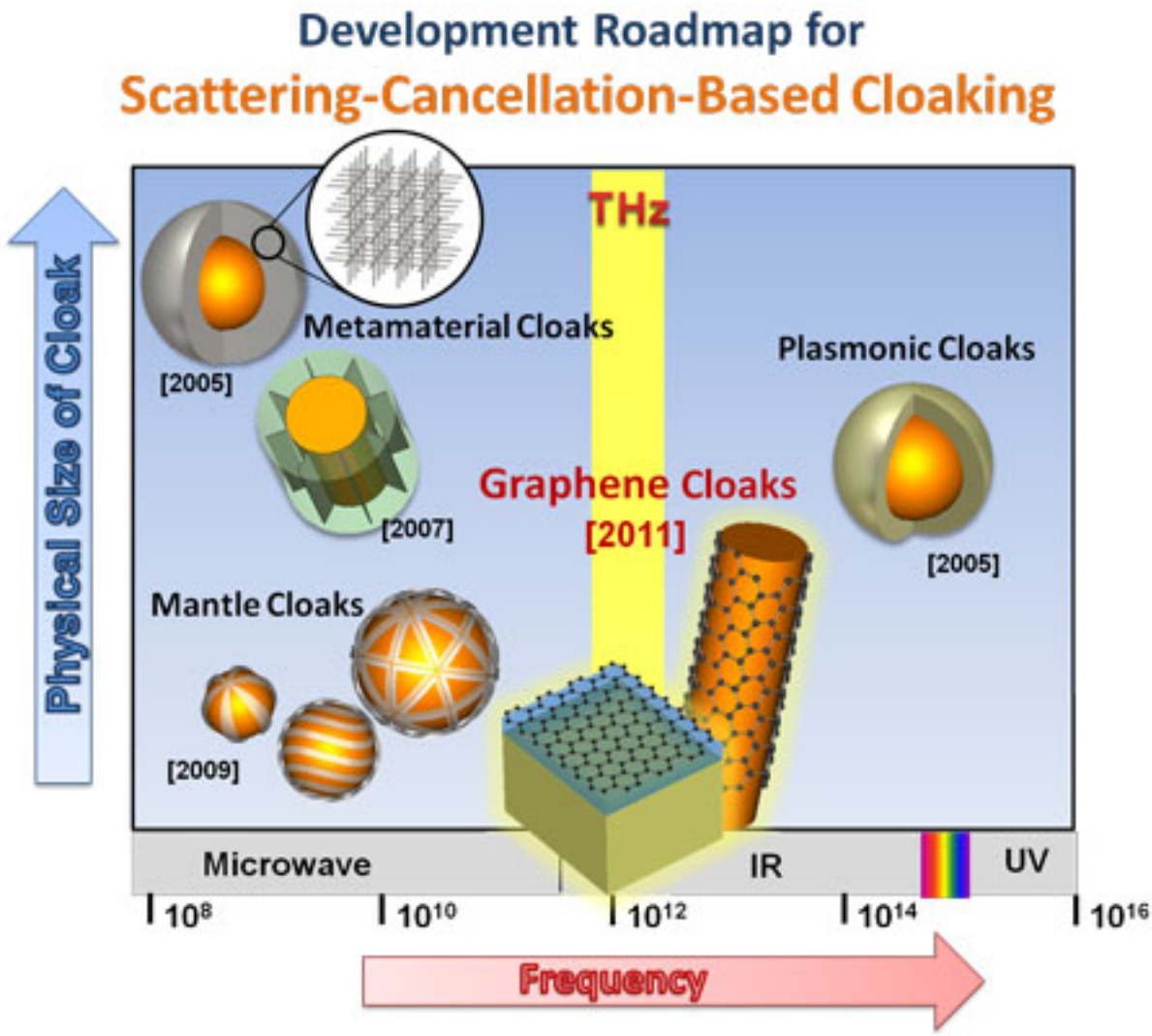
Graphene Enables Invisibility Cloak
**POSTED BY:** DEXTER JOHNSON / THU, JULY 07, 2011

Fans of the original Star Trek television show surely recall those dastardly Klingons employing a cloaking device that rendered their vessels invisible. Of course, that is science fiction, but in research coming out of the University of Texas at Austin that capability sounds amusingly similar to a proposed use of graphene in providing an “active, dynamically tunable invisibility cloak”.

The research, which was originally published in the ACS journal *Nano*, builds on two fields of previous work. The fist field is termed “plasmonic cloaking”, which uses metamaterial coatings, and the second is known as “mantle cloaking”, which achieves more or less the same effects as plasmonic cloaking but by using impedance.

"The graphene cloak idea stems from the mantle cloaking concept, which we have proposed at microwaves using frequency-selective surfaces, i.e., properly patterned conducting surfaces that can tailor their effective surface impedance at will," says Andrea Alùn, at The University of Texas at Austin, in the Nanowerk article cited above.

# Graphene Enables Invisibility Cloak




Alùn adds, “"Due to the recent progress in understanding graphene's AC conductivity, we have realized that its unique features of ultra-high mobility and largely tunable Fermi level may naturally provide the required reactive properties in a single atomic layer. The effective surface impedance of graphene can be tuned in real-time, another great advantage of this graphene cloak, which makes dynamically tunable and switchable cloaking operation possible."

While invisible aircraft may leap to mind, the applications for this technology could be in the areas of non-invasive sensors and low-scattering electronic components.

"There is great interest in realizing low-scattering or impedance-matched electronic components, and we believe that the use of this graphene layer may realize this effect in an ultrathin geometry – much thinner than anti-reflection coatings or other available

technology," says Alùn.

JULY 4, 2011 4:00 AM PDT

## The secret life of white-space radio

by Rupert Goodwins

Tim Newton of Neul--the company running the radio side of the white-space trials in the U.K.'s Bute and Cambridge--detailed the engineering challenges of the task when he spoke at the Future of Wireless conference in late June.

His thesis (PDF)--that the radio world white-space systems inhabit is very different to that of classic wireless engineering, and much novel thinking is needed--raised some interesting and important points.
The theory behind white-space wireless is simple. In order to avoid interference, TV transmitters on a common frequency are always geographically distant from each other, leaving the channel unused over much of the intervening land. As TV frequencies are particularly useful--combining good in-building penetration, copious bandwidth, decent range and small antennas--the thinking goes that whole new data services can be rolled out in those gaps, known as white space. To do this, the frequencies need to be carefully interleaved with the TV transmitters and low power used to prevent interference.

**The difficult part**

It's a powerful concept. The side that sounds difficult--making sure that the white-space systems are properly configured to work alongside the complex interlocking channel allocations of the TV stations--isn't so hard. White-space systems have GPS and every couple of hours interrogate a central database that tells them what frequencies to use: they can also easily refuse to initialize if they detect a strong, unexpected TV station where it's not expected.

The main problem with white space is that despite the maps, it's not white.
In classical radio theory, a receiver tuned to an empty channel picks up random noise that's primarily generated by thermal effects within the receiver, the antenna and the surroundings. Everything that's above absolute zero creates some electromagnetic noise by the random movement of electrons, and it's this very well modeled and understood effect that puts limits on the lowest strength signal you can pick up.
This isn't true for the TV bands in which white-space systems play. Although the transmitter coverage maps for TV stations seem to show large areas of the U.K. blank for each channel, this is only true if you're trying to pick up enough signal to create a watchable picture. Detectable signals turn up much further afield than the maps suggest.

For a start, the TV transmitters themselves are very powerful. Each digital multiplex can be up to 250KW, and there will be six multiplexes per site, with plans for a further two.

That's two megawatts from the strongest transmitters. Furthermore, the antennas are perched on top of very tall masts, giving them line of sight to horizons that can be 100km away. Even beyond those horizons, the transmissions refract over the edge of the Earth and can be detected well beyond that limit.

The result is that for almost every part of the U.K., in almost every channel, there are detectable signals from distant transmitters that the white-space system must overcome. And adding to the fun, the local TV transmissions are very strong.

**Mixed signals**

One of the hardest parts of radio design is preventing very strong signals from mixing with each other and creating internal interference in the initial stages of the receiver. One of the normal tricks for avoiding this is to make the receiver slightly deaf, perhaps increasing the strength of the transmitter it's picking up to compensate, but neither is an option for white-space radio. Thus, the receiver design must be excellent and use top-quality components.

That's rather ironic, as one of the absolute rules for white-space radio is that it mustn't interfere with TV reception--and TVs tend to have some of the worst radio circuits ever perpetrated on the public. Built to a price and with maximum flexibility taking precedence over high performance, TVs are liable to interference from perfectly well-behaved transmitters. That means white-space systems have to use as low a power as possible, even though they'll operate on unused local frequencies.

The final source of noise is gadget-based. All digital electronic equipment emits some radio signals, and various standards exist to minimize the interference this causes. However, there's a lot of it about, as you can easily hear if you hold a radio tuned to a dead channel close to a laptop, network wiring, Wi-Fi router, or other gizmo. Devices such as powerline networks and DSL modems use radio-frequency signals to carry data, and are particularly promiscuous in their emissions.

Again, if you're a TV station or a mobile phone company, you can in general set your transmission level to overcome the low-level interference from all these factors; it's your radio channel. White-space systems can't do that.

**Be clever**

The answer is to be clever: analyze the noise, find out what's causing it, and work around it. One technique is called kurtotic analysis. In effect, this looks for the characteristic spikes in energy that fingerprint a transmission that may be too weak to decode but is nevertheless strong enough to be a problem.

Digital TV transmissions are very well characterized, and there's a good chance that in

the future it'll be practical to mathematically cancel them out in the receiver. Currently, it's too computationally intensive to implement economically, but Moore's Law may fix that.

It's a mark of Neul's confidence in its radio technology that despite this hostile radio environment, it reckons it can cover well over 99 percent of the U.K. population with between 4,000 and 5,000 base stations. A lot depends on the field trials, though: it's not surprising that the first one was in the radio wastelands of the remote Scottish Isle of Bute. The second, in Cambridge, will be more interesting.