

Index

Cyber Bytes - 23 FEB 11

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

Links of interest:

Recent links of interest:

Qwiki (alternative to textual search; provides video & voice search results): <http://www.qwiki.com>

World IPv6 Day (6.08.2011): <http://isoc.org/wp/worldipv6day/>

IPv6 Readiness Page (to test your networks readiness): <http://www.test-ipv6.com/>

Art Project by Google (online art museums): <http://www.googleartproject.com>

Wi-Fi Alliance Urges Use of WPA2 encryption (podcast): http://news.cnet.com/8301-19518_3-20030160-238.html?part=rss&subj=news&tag=2547-1_3-0-20

IBM Watson Special on NOVA (the state of artificial intelligence) (video): <http://www.pbs.org/wgbh/nova/tech/smarter-machine-on-earth.html>

IBM Watson Takes a Job on Conan's Show (video): http://news.cnet.com/8301-17852_3-20032645-71.html?part=rss&subj=news&tag=2547-1_3-0-20

Federal R&D Dashboard: <http://rd-dashboard.nitrd.gov/>

Federal IT Dashboard: <http://it.usaspending.gov/>

Cloud Computing

IBM Researchers Back Homomorphic Crypto for Cloud Computing
- <http://news.techworld.com/security/3259753/ibm-researchers-back-homomorphic-crypto-for-cloud-computing/>

Pentagon Looks to Militarize the Cloud
- <http://www.wired.com/dangerroom/2011/02/pentagon-cloud/>

Cyber Security

Index

.mil Websites Down After Listed for Sale by Hacker

- <http://www.fiercegovernmentit.com/story/mil-websites-down-after-listed-sale-hacker/2011-01-23?utm_medium=rss&utm_source=rss>

Intel Developing Security 'Game-Changer'

- <http://www.computerworld.com/s/article/9206366/Intel_developing_security_game_changer_>

At Facebook, Defense Is Offense

- <http://news.cnet.com/8301-27080_3-20029954-245.html?part=rss&tag=feed&subj=News-Security>

DARPA Seeks Security Expertise From a Nontraditional Source: the Hacker Community

- <http://www.nextgov.com/nextgov/ng_20110204_8476.php>

NASDAQ Hackers Target Service for Corporate Boards

- <<http://www.npr.org/2011/02/05/133520004/report-hackers-penetrated-nasdaq-stock-market?ft=1&f=1001>>

NSA Chief Wants to Protect Private 'Critical' Networks

- <http://news.cnet.com/8301-31921_3-20033126-281.html?part=rss&subj=news&tag=2547-1_3-0-20>

Defense Is Building a Database to Analyze All Internet Traffic

- <http://www.nextgov.com/nextgov/ng_20110127_9318.php>

Cyber War

US Has Secret Tools to Force Internet on Dictators

- <http://www.wired.com/dangerroom/2011/02/secret-tools-force-net/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+wired%2Findex+%28Wired%3A+Index+3+%28Top+Stories+2%29%29>

The Cyberweapon That Could Take Down the Internet

- <<http://www.newscientist.com/article/dn20113-the-cyberweapon-that-could-take-down-the-internet.html>>

Too Much Hysteria Over Cyber Attacks

- <<http://www.google.com/hostednews/afp/article/ALeqM5h3t3G2Y3al5Pj3HTwJvgddamhICA?docId=CNG.68fd3cfd2282503c7edd2edbea786e20.8c1>>

Index

DOD

Navy Strengthens IT Capabilities Across Fleet

Actionable Intelligence

- <<http://www.seapower-digital.com/seapower/spsample/#pg16>>

Interview with Rear Admiral Gretchen Herbert

- <<http://www.seapower-digital.com/seapower/spsample/#pg36>>

US Military Says Keeps Up With China; Is it enough?

- <<http://www.reuters.com/article/2011/02/01/us-usa-china-military-idUSTRE7101AG20110201>>

Air Force Grapples with Bandwidth and Workforce Shortages

- <http://www.fiercegovernmentit.com/story/air-force-grapples-bandwidth-and-workforce-shortages/2011-02-07?utm_medium=rss&utm_source=rss>

Cybersecurity Runs Deep in Fiscal 2012 Budget Request

- <http://www.fiercegovernmentit.com/story/cybersecurity-runs-deep-fiscal-2012-budget-request/2011-02-16?utm_medium=rss&utm_source=rss>

Information & Society

The Inside Story of How Facebook Responded to Tunisian Hacks

- <<http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/>>

There's No Such Thing as 'Social Media Revolution'

- <http://news.cnet.com/8301-13577_3-20029519-36.html?part=rss&subj=news&tag=2547-1_3-0-20>

Social Media Revolution Hits Saudi Arabia

- <<http://www.npr.org/2011/01/26/133212623/social-media-revolution-hits-saudi-arabia?ft=1&f=1001>>

Can Governments Really 'Block' Twitter?

- <http://www.foreignpolicy.com/articles/2011/01/26/can_governments_really_block_twitter>

Index

The Internet Dies in Egypt

- <<http://networkeffect.allthingsd.com/20110128/the-internet-dies-in-egypt-in-pictures/>>

Egypt's Web, Mobile Communications Severed

- <http://online.wsj.com/article/SB10001424052748703956604576109661160604954.html?mod=WSJ_Tech_LEADSecond>

Egypt's Leaders Found 'Off' Switch for the Internet

- <<http://www.nytimes.com/2011/02/16/technology/16internet.html?partner=rss&emc=rss>>

Wary of Egypt Unrest, China Sensors Web

- <<http://www.nytimes.com/2011/02/01/world/asia/01beijing.html?partner=rss&emc=rss>>

Where Innovation Is Sorely Needed [Pervasive data and its impact to business models]

- <<http://www.technologyreview.com/business/32245/?ref=rss>>

Four Principles for Crafting Your Innovation Strategy

- <<http://www.technologyreview.com/business/32246/page1/>>

Social Surveillance Yields Smarter Directions [Use of social media for traffic advice]

- <<http://www.technologyreview.com/computing/32250/?ref=rss&a=f>>

Can Social Networking Keep Kids in School? [School-based Facebook]

- <<http://www.npr.org/2011/02/09/133598049/can-social-networking-keep-students-in-school?ft=1&f=1001>>

Information Technology

A Year Later, Microsoft Picture Looks Very Different

- <<http://www.reuters.com/article/idUSTRE70P0N020110126>>

Why the Entire Internet Is about to Become 'Slower and Flakier' [Exhausting IPv4 address space]

- <<http://www.technologyreview.com/blog/mimssbits/26297/?ref=rss>>

To Avert Internet Crisis, the IPv6 Scramble Begins

- <http://news.cnet.com/8301-30685_3-20029721-264.html?part=rss&subj=news&tag=2547-1_3-0-20>

Index

Drumming Up for Addresses on the Internet

- <http://www.nytimes.com/2011/02/15/technology/15internet.html?_r=1>

No Easy Fix as Internet Runs Out of Addresses

- <<http://www.wired.com/epicenter/2011/02/internet-addresses/all/1>>

US Puts End to India Export Restrictions

- <<http://www.defensenews.com/story.php?i=5542519&c=POL&s=TOP>>

FCC Takes Steps to Free Up Wireless Spectrum

- <http://news.cnet.com/8301-30686_3-20029841-266.html?part=rss&subj=news&tag=2547-1_3-0-20>

Intel's Sandy Bridge Chipset Flaw: The Fallout

- <http://news.cnet.com/8301-13924_3-20030070-64.html?part=rss&subj=news&tag=2547-1_3-0-20>

Battling a Wireless Deluge

- <http://online.wsj.com/article/SB10001424052748704124504576118353354099780.html?mod=WSJ_Tech_LEFTTopNews>

US Seeks Veto Powers Over New Domain Names

- <http://news.cnet.com/8301-31921_3-20030809-281.html?part=rss&subj=news&tag=2547-1_3-0-20>

Using IT to Drive Innovation

- <<http://www.technologyreview.com/business/32301/?ref=rss>>

Exabytes: Documenting the 'Digital Age' and Huge Growth in Computing Capacity

- <<http://www.washingtonpost.com/wp-dyn/content/article/2011/02/10/AR2011021004916.html>>

Behind the Information Overload Hype

- <<http://online.wsj.com/article/SB10001424052748704900004576152384123140652.html>>

Robotics

Cloud Robotics: Connect to the Cloud, Robots Get Smarter

- <<http://spectrum.ieee.org/automaton/robotics/robotics-software/cloud-robotics?>>

Index

utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+l33tSpectrum+%28IEEE+Spectrum%29>

Gorgon Stare Blinks a Lot; Testers Say Don't Field 'til Fixed
- <<http://www.dodbuzz.com/2011/01/24/gordon-stare-blinks-a-lot-testers-say-dont-field-til-fixed/>>

Air Force's 'All Seeing Eye' Flops Vision Test
- <<http://www.wired.com/dangerroom/2011/01/air-forces-all-seeing-eye-flops-vision-test/>>

X-47B Robot Stealth Plane Makes First Flight [Video at site below]
- <http://news.cnet.com/8301-17938_105-20030832-1.html?part=rss&subj=news&tag=2547-1_3-0-20>

Drone Will Call Aircraft Carriers Home
- <<http://online.wsj.com/article/SB10001424052748703507804576130493035362556.html>>

After Successful First Flight, Navy Plans for Next Stage of UCAS-D Development

US Navy Looks to Expand Unmanned Systems
- <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2011/02/04/01.xml>

Fire Scout to Gather Intel, Hunt Pirates
- <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awst/2011/02/07/AW_02_07_2011_p31-286989.xml&headline=Fire%20Scout%20To%20Gather%20Intel,%20Hunt%20Pirates>

Space

How to Hitch a Ride to Space (for your satellite)
- <http://news.cnet.com/8301-19882_3-20029400-250.html?part=rss&subj=news&tag=2547-1_3-0-20>

Weather Sat Program Slammed
- <<http://www.dodbuzz.com/2011/02/01/weather-sat-program-slammed/>>

Russia Loses Military Satellite
- <<http://www.defensenews.com/story.php?i=5593198&c=POL&s=TOP>>

Index

China Develops Counterspace Weapons

- <<http://www.defensenews.com/story.php?i=5625257&c=AIR&s=TOP>>

Technology Advances

'Universal' Memory Aims to Replace Flash and DRAM

- <<http://www.kurzweilai.net/universal-memory-aims-to-replace-flash-and-dram>>

Micron to Reveal Tech It Says Increases Chip Speed 2-Fold

- <http://news.cnet.com/8301-13924_3-20031380-64.html?part=rss&tag=feed&subj=News-CuttingEdge>

NAVAIR Working with Army to Develop New Wide-Area Surveillance Capability

Next Generation Super Computers

- <<http://spectrum.ieee.org/computing/hardware/nextgeneration-supercomputers/0>>

The Next Graphene?

- <<http://www.technologyreview.com/computing/32283/?ref=rss&a=f>>

Carnegie Mellon Assisting IBM's "Watson" with Machine Learning

- <http://www.cmu.edu/news/archive/2011/February/feb11_watson.shtml>

What IBM's Watson Tells Us About the State of AI

- <http://news.cnet.com/8301-13556_3-20031781-61.html?part=rss&subj=news&tag=2547-1_3-0-20>

A Fight to Win the Future: Computers vs. Humans

- <<http://www.nytimes.com/2011/02/15/science/15essay.html>>

For Watson Technology, What Happens After 'Jeopardy!'?

- <<http://abcnews.go.com/Technology/watson-technology-jeopardy/story?id=12869629>>

Laser-Quick Data Transfer [Lasers on silicon]

- <<http://www.technologyreview.com/computing/32324/?ref=rss>>

Stanford Researchers Develop Wireless Technology for Faster, More Efficient Communications Networks

- <<http://news.stanford.edu/news/2011/february/duplex-radio-transmission-021411.html>>

Index

Researchers Detail Programmable Nanoprocessor

- <<http://www.zdnet.co.uk/news/emerging-tech/2011/02/11/researchers-detail-programmable-nanoprocessor-40091770/?tag=mncol;txt>>

The Smallest Computing Systems Yet

- <<http://www.technologyreview.com/computing/32302/?ref=rss&a=f>>

New Anti-Laser Tech Paves Way for Optical Computing

- <<http://www.infoworld.com/d/hardware/new-anti-laser-tech-paves-way-optical-computing-114>>

IBM Researchers Back Homomorphic Crypto for Cloud Computing

[IBM researchers back homomorphic crypto for cloud computing](#)

Encrypted blobs can be processed without decryption

By Ellen Messmer | [Network World US](#)

Published: 11:15 GMT, 07 February 11

Can cloud-based computing be made more secure in the future using what crypto geeks call "fully homomorphic encryption" to send data as "encrypted blobs" that can be understood and subject to processing without having to actually de-crypt them first to see the plaintext?

"That's the vision," says JR Rao, IBM's senior manager for secure software and services at the IBM Thomas J Watson Research Centre. He notes that breakthrough mathematical work in fully homomorphic encryption done by IBM researcher [Craig Gentry](#) is providing a "foundation for the encrypted path" that IBM hopes will radically improve how data can be kept secret and confidential.

But Rao acknowledges the feeling that it's all still a bit like the Wright brothers' first flight in aviation, with some practical developments needed before everyone climbs on board.

Today, data can be encrypted using a variety of techniques, but in order to do anything that might have to be done with the data, it's necessary to decrypt it. "Today, to work with data, you have to work with data in the clear," Rao notes. "And that can be a problem."

Instead, the idea is to create "encrypted blobs" that don't have to be decrypted and still allow for many practical applications by being combined with and processed by other encrypted blobs. "But you know what's encrypted in the blobs," says Rao.

But others don't. With what has been ground-breaking development work in fully homomorphic encryption, it's possible.

IBM is convinced the basis is there to do a wide variety of things with encrypted blobs, including computational arithmetic on encrypted data, which

IBM Researchers Back Homomorphic Crypto for Cloud Computing

could be useful in the financial sector. Or privacy-enhancement for web services such as searching, which would keep search engines from building up profiles on people. And in cloud computing, it would be a way to store data so that there could be authorised processing of it without it having to be changed into cleartext and then encrypted again.

"We're in the process of working on that now," says Rao. The goal is that "if end users are submitting private and sensitive information in the cloud," they would know that data would be kept confidential as encrypted blobs. "We're now figuring out how to do this in cloud computing," he says, but adds that IBM is not at the stage to announce products or services yet.

Pentagon Looks to Militarize the Cloud

Pentagon Looks to Militarize the Cloud

- By [Spencer Ackerman](#)  February 22, 2011 | 7:00 am | Categories: [DarpaWatch](#)

Store tactical military data on distributed servers, accessible through networked computers or mobile devices? Ask most officers about cloud computing and they'll look at you patronizingly and say: *Yes, Google Docs is nice, but it's not secure enough for our secrets.* (I write from experience.) But Darpa's [new budget](#) shows that it wants the military all the way up into the cloud, and plans to set up mobile wireless hotspots so troops can reach the cloud from the most connectivity-forsaken places.

Appropriately, the goal of getting big data files to troops on the move in the middle of nowhere is, well, distributed between two new programs from the Pentagon's blue-sky researchers. Cloud to the Edge looks to essentially ape Google's tools (other than search) to create a military cloud. And Mobile Hot Spots wants to carry connectivity anywhere troops need to share those big data files.

Wherever the military goes, it [brings bandwidth](#) with it. But it's easier to set up networks around big bases than it is to have them follow troops in the field, especially if those troops have to send or receive large data packets, like video from drones overhead. Some companies are combating the problem by [mounting cell towers under the bellies of drones](#), beaming connectivity below.

Mobile Hot Spots is Darpa's way to even out what it calls the "100-1000x mismatch of data needs and available network capacity." Starting out with a \$10 million request to Congress, it looks to "create high-capacity and secure wireless technologies by exploiting advances in high-frequency and new security paradigms using RF, millimeter wave (MMW) and/or optical transmission." If approved, it'll spend its first year of life developing hardware and network architecture for the mission. And it's considering going the under-drone route, proposing to "explore hardware, software, and waveform options to include unmanned aerial systems, soldiers, and mobile

Pentagon Looks to Militarize the Cloud

platforms connected into network topologies.”

Then there’s the place where the data carried over those networks will reside. Cloud to the Edge has no problem distributing that around through the ether. Unlike Mobile Hot Spots, it’s not even asking for money yet — perhaps because what it’s proposing is so ambitious it first needs to see about feasibility. Not only will it store data in “distributed servers and advanced networking and information database technologies,” it seeks to minimize human interaction in retrieving the data, “autonomously seek[ing] out relevant information and mov[ing] it to where it is needed in a timely and assured manner.”

The budget proposal doesn’t give any hint about how it’ll do that yet, proposing for now just to study “information flow patterns through the regional and localized network” and write software for “distributed data dissemination.”

Neither does Darpa explain how to keep its Cloud secure. Instead, it flips the security question back around, asserting that the “current centralized or regional storage and dissemination of information presents security, reliability, and capacity challenges in identifying and getting relevant information to users at the edge.”

At a time when Special Operations Forces are turning to [Android-powered tablets](#) to read their data in the middle of nowhere, Darpa looks to be focused on setting up the supporting infrastructure that lets U.S. troops access more information in more remote areas. It might not be Google Docs. But it’s something.

.mil Websites Down After Listed for Sale by Hacker

.mil websites down after listed for sale by hacker

January 23, 2011 — 9:08pm ET | By [David Perera](#)

A hacker has apparently been selling administrative control of military websites online for as little as \$399, says cybersecurity vendor Imperva.

In a Jan. 21 post on the company's [blog](#), Imperva has redacted screenshots of websites a hacker says he has compromised along with the price of "FullSiteAdmin Control."

Cybersecurity blogger Brian Krebs has a considerably less redacted screenshot on his [blog](#). "I've seen some of the back-end evidence of his hacks, so it doesn't seem like he's making this up," Krebs adds.

Among the websites listed for sale is <http://cecom.army.mil/>, the website of the Army's Communications Electronics Command, for \$499. On Jan. 23, the site was mostly offline ([click for a screenshot](#)), simply displaying a html message that "cecom.army.mil Is Temporarily Unavailable We're working to resolve this issue."

Also offline was <http://pec.ha.osd.mil> ([click for a screenshot](#)), the website for Department of Defense the PharmacoEconomic Center, which displayed the same html message as the CECOM website. The hacker had listed control of it for sale for \$499.

Another military website on the list, www.scguard.army.mil, the website of the South Carolina National Guard, was totally offline Jan. 23, the URL returning a 403 Forbidden status code ([click for a screenshot](#)). Of the military websites listed for sale by the hacker, the site was the relative bargain at \$399 for full control.

Cheaper wares included www.utah.gov for \$99 (the website appeared to be working normally on Jan. 23) and MySQL root access to <http://michigan.gov> (also up and running) for \$55.

The hacker also has offered for sale personally identifiable information from hacked websites, including government websites, at \$20 per thousand records, according to Imperva.

Krebs notes that the DoD's PharmacoEconomic Center would be an attractive site for rogue online pharmacies to plant links on, since search engines give links from .mil, .gov and .edu sites more authority than other links from top level domains.

.mil Websites Down After Listed for Sale by Hacker

Intel Developing Security 'Game-Changer'

Intel developing security 'game-changer'

Intel CTO says new technology will stop zero-day attacks in their tracks

By Sharon Gaudin

January 26, 2011 06:00 AM ET

Computerworld - Intel's chief technology officer says the chip maker is developing a technology that will be a security game changer.

[Justin Rattner](#) told *Computerworld* on Tuesday that scientists at [Intel](#) are working on [security](#) technology that will stop all zero-day attacks. And, while he would give few details about it, he said he hopes the new technology will be ready to be released this year.

"I think we have some real breakthrough ideas about changing the game in terms of malware," Rattner said. "We're going to see a quantum jump in the ability of future devices, be them PCs or phones or tablets or smart TVs, to defend themselves against attacks."

He noted that the technology won't be signature-based, like so much security is today. Signature-based malware detection is based on searching for known patterns within malicious code. The problem, though, is that zero-day, or brand-new, malware attacks are often successful because they have no known signatures to guard against.

[Intel](#) is working around this problem by not depending on signatures.

And the technology will be hardware based, though it's still unclear if it will have a software component.

Intel Developing Security 'Game-Changer'

"Right now, anti-malware depends on signatures, so if you haven't seen the attack before, it goes right past you unnoticed," said Rattner, who called the technology "radically different".

"We've found a new approach that stops the most virulent attacks. It will stop zero-day scenarios. Even if we've never seen it, we can stop it dead in its tracks," he said.

Dan Olds, an analyst with The Gabriel Consulting Group, said if this technology works as Rattner says it will, it could be a major advance for computer security.

"If Intel has hardware technology that can reliably stop zero-day attacks, that would be a huge win in the war against malware," Olds said. "The key is that it's reliable. It has to have the ability to discern legit software from malware. But if they can pull this off, it would give them quite a competitive advantage [vs. AMD](#)."

And Olds noted that technology that takes advantage of hardware could be interesting.

"The best security is a combination of hardware and software," he said. "Hardware security can be stronger and faster in some situations, but isn't as flexible as software-only mechanisms. The big change here is that it sounds like Intel is pulling security functions into the chip or the chipset."

Rattner said Intel researchers were working on the new security technology before the company moved to [buy security software maker McAfee](#). However, he said that doesn't mean that McAfee might not somehow be involved.

With that \$7.68 billion deal, Intel will become more than just a chip maker. It will

Intel Developing Security 'Game-Changer'

become a security company, as well.

At Facebook, Defense Is Offense

At Facebook, defense is offense

by Elinor Mills

PALO ALTO, Calif.--The nerve center for Facebook's security team is a room tucked away on the lower level of the company's main building here. The word *scalps* is painted in big blue stenciled letters on the back wall, which serves as a kind of scrapbook of legal and other wins for the social-networking company.

Taped to the wall are photos of spammers getting served notices of lawsuits, copies of checks defendants have used to settle suits filed by Facebook, mug shots of child predators who were kicked off the site and face criminal charges, cease and desist letters sent to fraudsters who sold fake Facebook accounts, and a letter from a former spam-happy teenager that starts "I appreciate that you spoke to my mom."

The wall of scalps is a source of pride for Facebook's security team and is representative of the company's aggressive, no-holds-barred approach to keeping fraudsters and thieves away from its more than 500 million users.

"We've built an offensive capability," says Joe Sullivan, chief security officer at Facebook. "Filing civil lawsuits is not a PR statement; it's very impactful. We monitor underground forums and the spammers discuss the judgments. It has a deterrent effect."

Indeed, settlement judgments--including the \$873 million record judgment in [one Facebook case](#)--aren't something to sniff at if you're in it for the money.

Facebook's litigiousness should come as no surprise given Sullivan's background. He joined Facebook in 2008 after working in various security and legal roles at PayPal and eBay for six years and at the U.S. Department of Justice for eight years. He was the first federal prosecutor in a U.S. Attorneys' office working full-time on high-tech crime cases and was a founding member of the Computer Hacking and Intellectual Property Unit in Silicon Valley. Recently, he joined the board of the [National Cyber Security Alliance](#).

"The philosophy predates me, but it's one I'm excited to be a part of," Sullivan told CNET in a recent interview. "You can't just build walls. You have to create incentives for people to not want to cause trouble."

Tunisian passwords

Lately, in addition to trying to keep the bad guys off of Facebook, Sullivan and his team have had to thwart outside attempts to keep some users from the site.

On Christmas Day, the security staff started hearing complaints from political activists in Tunisia--who had been protesting against the government since December--that their Facebook accounts

At Facebook, Defense Is Offense

were being compromised. It turned out that Internet Service Providers in that country were injecting malicious code into the Facebook log-in pages that was hijacking users' passwords as they tried to get onto the site, Sullivan said.

"We had to figure out how we could stop this technical attack quickly without breaking the Web site for everyone," he said. "This is the fun part of our job. We get to react to things that no one has dealt with before. Nobody freaked out."

After conferring with tech-savvy representatives from nongovernmental organizations, the U.S. government, and others, Facebook came up with a solution to fix the problem and began rolling it out to users in Tunisia over the next week. After that, the site saw a 15 percent jump in traffic from that country, according to Sullivan.

"We're not getting involved in geopolitical debates," he said. "We're just protecting our users." That's not the only time the popular social-networking site has found itself in the crossfire between people using the Internet to plan protests and spread information and governments that want to stop them.

Last week, the site reported service disruptions and a drop in traffic from Egypt, where protesters were demanding an end to the 30-year reign of President Hosni Mubarak. And in 2009, Iranians relied on Facebook (and Twitter and YouTube) during antigovernment street protests amid a text messaging and cell phone blackout.

A few months ago, Facebook found itself dealing with another politically sensitive matter when an ISP in a South Asian country that Sullivan declined to name appeared to be doing something fishy. Random pages were popping up on the site for people accessing Facebook from that country.

"One of the largest ISPS in that country was clearly using filtering software directed by the government," Sullivan said. "It broke the Facebook experience by caching the wrong information."

So, Facebook blocked that ISP and told the company it wouldn't allow access to the site until the problem was fixed. "You hear of countries blocking sites like Facebook. Well, sometimes we block them too," Sullivan said.

"We make a judgment call on how to best protect our users. We're not thinking of it from a political standpoint," he said. "We do get lawful government data requests and work with our lawyers on those. But where there is a risk of exposure of (customer) information outside that process, we want to prevent that."

Malware and phishing road blocks

The cases involving governments are few and far between, however. Ninety percent of the time the Facebook security engineers are just trying to prevent financially motivated scammers from taking

At Facebook, Defense Is Offense

over user accounts and distributing spam. Overseeing the technical end of that effort for Facebook is Ryan McGeehan, security manager for incident response.

McGeehan, who used to work on Web security for the Federal Reserve Bank and volunteers for the [Honeynet Project](#) security research nonprofit, tries to understand the mindset of attackers and anticipate what tricks they might try next.

As a result of his work with the Honeynet Project he is able to predict threats. For example, his team took advantage of a period when the Koobface worm was dormant to research antiphishing techniques before the malware starting attacking again, he said.

"Our detection (technology) had to change," McGeehan said. "We took older technologies and applied them to the malware."

Because account hijacking is so much of a problem due to increasingly clever phishing efforts, Facebook has advanced security features any user can enable and is turning to novel authentication methods for protecting at-risk accounts.

People can have Facebook notify them if their account is being accessed by a device the site does not recognize as being one they normally use. Users also have the option to see all the active sessions associated with their account and close ones they don't want open, from forgetting to log off at an Internet cafe, for example. People can ask the site to send them a onetime password for use on computers they don't trust. And [last week](#), Facebook began rolling out a feature that lets people use HTTPS (Hypertext Transfer Protocol Secure) encryption technology for all of their activity on Facebook, not just when they are typing in the password.

McGeehan's team has devised what it calls "roadblocks" when it detects anomalous activity that would indicate a possible malware infection on the computer or that someone other than the authorized account owner is trying to access the site. For example, if the system notices that an account is sending a large number of messages or making a lot of posts and posting dubious links--activities that could indicate a malware infection--the computer will direct the user to a free browser-based [McAfee Clean and Repair](#) tool that can be used immediately.

The company also is using "social authentication" to keep hijackers out of accounts even when they have the password. If the system doesn't recognize the device being used by a particular account to log in, or the location is new, it will force whoever is trying to access an account to prove he or she is the authorized account owner. If the account owner has provided Facebook with a mobile phone number, the system may send a code via text message that can be used to access the account. The person attempting to log in also may have to prove they are the owner of the account by matching names of Facebook friends with their photos as they are presented randomly.

"How do we recognize that the person logging in isn't you? Behind the scenes we have built a robust process to detect that, and we put the person through a flow that only the account owner" could navigate, said McGeehan, who has some patents pending related to the use of the "social

At Facebook, Defense Is Offense

graph."

Despite all the efforts, problems are bound to happen as they do at any big Internet Web site. [Last week](#), Facebook reported that a bug in an API (Application Programming Interface) allowed someone who was unauthorized to post to the Fan pages of company CEO Mark Zuckerberg and a couple of other unidentified high-profile accounts, which may or may not have included French President Nicolas Sarkozy's page.

"We have a history of being quick to act on any vulnerability we find," McGeehan said when asked to comment on the glitch. "This is something that separates us from other Web sites."

Privacy matters

A few security professionals who follow Facebook closely concurred with McGeehan's boast and, in general, praised the company's security efforts with regard to attacks on users or data from outside the site. However, several of them voiced concerns about privacy issues related to Facebook's policies and practices for data used for advertising and by third-party apps.

"Their track record has been good on internal security. There have been surprisingly few hacks on their system given the amount of attention they get," said Chester Wisniewski, senior security advisor at antivirus vendor Sophos. "The bigger picture of security at Facebook is how they're handling people targeting the users" by way of malicious or misleading apps distributed by fraudulent developers.

"They seem to be doing a reasonably good job of shutting these things down once they pop up, but what are they doing to prevent fraudulent apps from being created?" he said.

Asked whether and how Facebook vets the apps, Sullivan said: "We have a dedicated team and dedicated processes. What people sometimes misinterpret is that it is not an upfront gatekeeper (approach). It's a risk-based approach." Facebook's platform operations team doesn't scrutinize every single app, rather it devotes its energy to the ones that could cause the most damage if they were bad, he said.

"We look at and regularly review apps that are being used," Sullivan said. "Not ones that reached critical mass, but if they show any type of velocity. And velocity can be defined by sheer volume of users, publishing, (if they have) access to more than basic information, complaints."

Facebook also has reined in the ability of apps that formerly were unrestrained in the amount of information they had access to. Now, in order for an app to get access to data beyond what Facebook considers basic information needed for people to search for others on the site, the app must get explicit permission from the user. But Wisniewski said users should have the ability to pick and choose the access rights they want any particular app to have to their data.

"When it comes to privacy stuff they make you opt out, but when it comes to security you have to

At Facebook, Defense Is Offense

opt in," he said.

Asked to comment on the privacy concerns, Sullivan said there was a lot of misinformation about Facebook's marketing practices and that, for example, the company does not turn over user information to advertisers.

"Our objective is to give users choice and make sure that choice is transparent, and if a developer wants to say I need these 10 pieces of information for my application, you don't want to force the developer to change their product," he said. "We want to help the user make an informed decision about whether they want to share that information."

Ultimately, the debate centers on what trade-offs Facebook chooses to make to be able to keep growing the platform by attracting developers and ad revenue, and whether users are willing to accept those business decisions.

"Fundamentally, their business is advertising and targeted advertising based on your interest and your profile. Whatever data you upload to their site is grist for the mill so they can sell advertising," said Andrew Walls, a research director at research firm Gartner's security, risk, and privacy group. "They're doing a fair job of exploring the space between privacy expectations of consumers, the business needs of Facebook, and what society at large wants to see happen down the road."

DARPA Seeks Security Expertise From a Nontraditional Source: the Hacker Community

DARPA seeks security expertise from a nontraditional source: the hacker community

BY DAWN LIM 02/04/2011

The Defense Department plans to fund independent security researchers and experimental projects in a bid to invigorate the federal government's "unsustainable" approach to [cybersecurity](#), said Peiter "Mudge" Zatkó, a program manager at the Defense Advanced Research Projects Agency. Zatkó made the announcement Jan. 28 in a keynote speech at ShmooCon, an annual security research conference in Washington.

The program, called Cyber Fast Track, will reward security research done within "a matter of months and at a small price tag." Its emphasis on slimmer, unconventional solutions will rope in nontraditional players, such as hobbyists, startups and hacker spaces -- a term the security community uses in reference to technology-oriented collectives and experimental spaces, Zatkó said, in follow-up e-mail.

The program aims to implement cybersecurity projects faster, he said. Awardees would retain commercial rights over their work.

While not excluding traditional performers, such as research institutions, the program would support work that has been conducted mostly under the radar but is catching the eye of the government.

"Since the early '80s there has been some contingent of cyber researchers and hobbyists operating in low-budget settings," said Zatkó, formerly affiliated with the freewheeling Boston-based hacker collective [L0pht](#), known for its [1998 Senate testimony](#) that it could shut down the Internet in 30 minutes. The limited resources these groups operate on "forces them to be extremely creative," he said.

Yet it is "really painful" for small organizations to engage the government because its institutions have been "set up for multimillion-dollar, multiyear-long efforts," Zatkó said in his keynote. DARPA hopes the approach used with Cyber Fast Track can be applied elsewhere in Defense, he added.

Current cybersecurity strategy involves layering costly defensive security applications onto large IT infrastructures, which isn't sustainable, he said.

Total federal cybersecurity spending from 2010 to 2015 is expected to reach \$55 billion, according to a [forecast](#) by Market Research Media. The market for cybersecurity products is likely to grow to \$10 billion this year, an 11 percent increase from 2010, according to *Bloomberg Government*.

DARPA Seeks Security Expertise From a Nontraditional Source: the Hacker Community

Ramping up the use of defensive applications is a necessary means of "buying tactical breathing space," but it has proved, in some instances, counterproductive, Zatkan said.

A vulnerability watch-list created by Joint Task Force-Global Network Operations, now a wing of U.S. Cyber Command, showed that at one point, six of 17 vulnerabilities monitored by the task force could be traced to the security software itself being deployed to "fix" the system, such as antivirus suites.

DARPA research in environments the agency had access to found that defensive applications took up 10 million lines of code, compared to 125 lines of code found in 9,000 samples of malware.

Lines of code are an indication of the exploitable surface area of a system and the cost required to maintain and protect it. An IBM metric suggests that for every 1,000 lines of code, one to five bugs are introduced.

"You're spending all this effort layering on all this extra security," Zatkan said, "and it turns out that's introducing more vulnerabilities."

Federal requirements to create uniform systems amplifies the chances that bugs are reproduced across all the systems sharing those features, he said, highlighting an OMB [mandate](#) that called for agencies to standardize their use of Windows-operated systems.

Addressing the ShmooCon crowd, which he referred to as "the community that I came from [and] I still relate to," Zatkan said, "I want you guys to stay like you are. You are more valuable doing the kind of work that you're doing the way you're doing it now."

NASDAQ Hackers Target Service for Corporate Boards

Nasdaq Hackers Target Service For Corporate Boards

by THE ASSOCIATED PRESS

February 5, 2011

The company that runs the Nasdaq stock market said Saturday that hackers had penetrated a service that handles confidential communications between public companies and their boards.

The service run by [Nasdaq OMX Group Inc.](#) carries strategic information for about 300 companies. The company said it appears no customer data was compromised.

Nasdaq OMX said the hacking attempts did not affect its trading systems. Nasdaq is the largest electronic securities trading market in the U.S. with more than 2,800 listed companies.

The targeted application, Directors Desk, is designed to make it easier for companies to share documents with directors between scheduled board meetings. It also allows online discussions and Web conferencing within a board.

Since board directors have access to information at the highest level of a company, penetrating the service could be of great value for insider trading. The application's Web page says "Directors Desk provides multiple layers of security to protect our clients' most vital corporate records."

A federal official tells The Associated Press that the hackers broke into the systems repeatedly over more than a year. Investigators are trying to identify the hackers, the official said. The motive is unknown. The official spoke on condition of anonymity because the inquiry by the FBI and Secret Service is continuing.

Nasdaq OMX spokesman Frank DeMaria said the Justice Department requested that the company keep silent about the intrusion until at least Feb. 14. However, *The Wall Street Journal* reported the investigation on its website late Friday, prompting Nasdaq

NASDAQ Hackers Target Service for Corporate Boards

to issue a statement and notify its customers.

DeMaria said Nasdaq OMX detected "suspicious files" during a regular security scan on U.S. servers unrelated to its trading systems and determined that Directors Desk was potentially affected. It pulled in forensic firms and federal law enforcement for an investigation, but found no evidence that any customer information was accessed by hackers.

Nasdaq acquired the company behind Directors Desk in 2007.

In 1999, hackers infiltrated the websites of Nasdaq and the American Stock Exchange leaving taunting messages, but Nasdaq officials said then that there was no evidence the break-ins affected financial data.

NSA Chief Wants to Protect Private 'Critical' Networks

NSA chief wants to protect 'critical' private networks

by Declan McCullagh

NSA chief Keith Alexander, who also runs the U.S. Cyber Command, says it's time to "refine the roles of government and the private sector in securing this nation's critical networks."

(Credit: Declan McCullagh/CNET)

SAN FRANCISCO--The head of the National Security Agency said today that the U.S. military should have the authority to defend "critical networks" from malware and other disruptions.

Gen. [Keith Alexander](#), who is also the head of the Pentagon's [U.S. Cyber Command](#), said at the RSA Conference here that the NSA's "active defenses" designed to defend military networks should be extended to civilian government agencies, and then key private-sector networks as well.

"I believe we have the talent to build a cyber-secure capability that protects our civil liberties and our privacy," Alexander said.

Alexander's comments come only two days after William Lynn, the deputy secretary of defense, [offered](#) the same suggestion. In an [essay](#) last year, Lynn likened active defenses to a cross between a "sentry" and a "sharpshooter" that can also "hunt within" a network for malicious code or an intruder who managed to penetrate the network's perimeter.

But the power to monitor civilian networks for bad behavior includes the ability to monitor in general, and it was the NSA that [ran](#) the controversial warrantless wiretapping program under the Bush administration. Concerns about privacy are likely to turn on the details, including the extent of the military's direct involvement, and whether Web sites like Google.com and Hotmail.com could be considered "critical" or the term would only be applied to facilities like the Hoover Dam.

Alexander offered little in the way of specifics today. "We need to continue to refine the roles of government and the private sector in securing this nation's critical networks," he said. "How do we extend this secure zone, if you will? How do we help protect the critical infrastructure, key resources?"

At the moment, the Department of Homeland Security has primary responsibility for [protecting](#) critical infrastructure. A presidential directive ([HSPD 7](#)) says the department will "serve as a focal point for the security of cyberspace." During an appearance at RSA two years ago, Alexander [stressed](#) that "we do not want to run cybersecurity for the U.S. government."

That was then. After Cyber Command was created--following [reports](#) of a power struggle between DHS and the NSA--it moved quickly to consolidate its authority. An October 2010 memorandum of agreement ([PDF](#)) between the two agencies says they agree to "provide mutually beneficial logistical and operational support" to one another.

NSA Chief Wants to Protect Private 'Critical' Networks

Senators Joseph Lieberman (I-Conn.) and Susan Collins (R-Maine) recently [pledged to reintroduce](#) a controversial bill handing President Obama power over privately owned computer systems during a "national cyberemergency," with limited judicial review. It's been called an Internet "kill switch" bill, especially after [Egypt did just that](#).

Alexander didn't address that point. "The intent would be: let's build how we can do this with DOD, show we can extend that to the government, and then to key critical infrastructure," he said.

Defense Is Building a Database to Analyze All Internet Traffic

Defense is building a database to analyze all network traffic

BY ALIYA STERNSTEIN 01/27/2011

The Defense Department is building a database to cull traffic from networks across government and other sectors, which will participate on a voluntary basis, to develop a fuller view of online threats, a top Defense official said.

U.S. Cyber Command, the Defense Department's new joint-service organization created primarily to protect military information networks, is still defining its role in the governmentwide effort to protect the Internet. Foremost, the organization wants to establish a common operational picture of cyberspace, said Marine Corps Lt. Gen. Robert E. Schmidle Jr., CYBERCOM's deputy commander.

"One of the things that I'm going to try to do is bring these data feeds in from all of the services, the agencies and anybody that comes to participate -- and that will be an ugly challenge," he said Wednesday at a seminar on [cybersecurity](#) regulation that the Potomac Institute for Policy Studies hosted.

In exchange for such cooperation, contributors would have access to the common database so that when incidents arise, the government can respond with a holistic approach, Schmidle explained.

Security experts have raised concerns about Defense poking too far into private sector and civilian agency networks. Former President George W. Bush gave the Homeland Security Department primary responsibility for cybersecurity. The military's involvement in commercial and civilian networks has become a hot-button issue in Washington, where lawmakers and senior federal officials continue to debate the best way for Defense to defend cyberspace without violating privacy.

Schmidle said the command supervises the operation of only websites carrying the .mil domain, defends that domain and -- when ordered by civilian authorities -- conducts offensive actions on the Internet. But he acknowledged the lines between defensive and offensive activities blur. "You can't do defensive operations effectively in cyberspace unless you are doing offensive operations -- unless you are out there hunting on networks," Schmidle said.

"In many cases, if you have your own network, you really want to have visibility over your network and somebody else's -- but you're not quite so sure you want to expose everything you do to someone else," he noted. "I think, in Cyber Command, in order for us to do this defense piece the way we need to be able to do it, we have to have visibility into these networks.

"One of the things that keeps me up at night is the nation's [critical infrastructure](#)," which Defense

Defense Is Building a Database to Analyze All Internet Traffic

works closely with DHS to protect, Schmidle said. Recently, the computer worm Stuxnet emerged as a potential threat to the operating systems that control electric grids, water pipelines and manufacturing plants.

Schmidle said he understands why some Americans might expect Defense to take charge of U.S. cybersecurity: "We've got a lot of the money and a lot of the resources, but that doesn't necessarily make it right."

An audience member said the common database Schmidle described brought to mind the WikiLeaks imbroglio, in which a soldier allegedly stole State Department diplomatic cables from an internal, information sharing network so he could leak the documents.

"The Internet was designed to be collaborative -- and yet we find that [the structure enabling collaboration], in terms of trying to defend the Internet, is one of the principle weaknesses," Schmidle responded. He said a solution might be user-defined information sharing, where networks are built in a way that segregates authorized users from unauthorized users.

The issue of insider threats came up several times on Wednesday.

When asked whether a Pearl Harbor-like event might transpire and, if so, whether it would be orchestrated by an American or a foreign entity, Schmidle said, "It certainly is conceivable that there could be an event that would get our attention in cyberspace." He said he was hesitant to predict its source, but "I think that we need to continue to be as sensitive to the potential for internal insider threats as we are upon other things."

US Has Secret Tools to Force Internet on Dictators

U.S. Has Secret Tools to Force Internet on Dictators

- By [Spencer Ackerman](#)  February 7, 2011 | 7:00 am | Categories: [Info War](#)

When Hosni Mubarak shut down Egypt's internet and cellphone communications, it seemed that all U.S. officials could do was ask him politely to change his mind. But the American military does have a second set of options, if it ever wants to force connectivity on a country against its ruler's wishes.

There's just one wrinkle. "It could be considered an act of war," says [John Arquilla, a leading military futurist](#).

The U.S. military has no shortage of devices — many of them classified — that could restore connectivity to a restive populace cut off from the outside world by its rulers. It's an attractive option for policymakers who want an option for future Egypts, between doing nothing and sending in the Marines. And it might give teeth to the Obama administration's demand that foreign governments consider [internet access an inviolable human right](#).

Arquilla, a professor at the Naval Postgraduate School, spent years urging the military to logic-bomb adversary websites, disrupt hostile online presences, and even cause communications blackouts to separate warring factions before they go nuclear. What the military can turn off, he says, it can also turn on — or at least fill dead airspace.

Consider the Commando Solo, the [Air Force's airborne broadcasting center](#). A revamped cargo plane, the Commando Solo beams out psychological operations in AM and FM for radio, and UHF and VHF for TV. Arquilla doesn't want to go into detail how the classified plane could get a denied internet up and running again, but if it flies over a bandwidth-denied area, suddenly your Wi-Fi bars will go back up to full strength.

"We have both satellite- and nonsatellite-based assets that can come in and provide

US Has Secret Tools to Force Internet on Dictators

access points to get people back online,” Arquilla says. “Some of it is done from ships. You could have a cyber version of pirate radio.”

Then there are cell towers in the sky. The military already uses its aircraft as communications relays in places like Afghanistan. Some companies are figuring out upgrades: FastCom, an effort led by the defense firm Textron, is a project that [hooks up cellular pods to the belly of a drone](#), the better to keep cellular and data connections in the air without pilot fatigue. Underneath the drones, a radius of a few kilometers on the ground would have 3G coverage.

Sharon Corona, a spokeswoman for the project, says that there’s an obstacle to using a technology like FastCom for an Egypt-like situation: The recipient devices need to be able to talk with the cell and data signal. But compliant phones or netbooks — small and lightweight — could conceivably be smuggled into a denied area.

Alternatively, operatives could smuggle small [satellite dishes into a country](#). Small dishes were crucial to [getting the internet back running in Haiti](#) after last year’s earthquake. It’s how cameramen in war zones rapidly transmit high quality video from the middle of nowhere.

Of course, slow-flying drones or a broadcasting center in the sky have an inherent weakness: They’re sitting ducks for any half-decent air defense system. (And did we mention that Hosni Mubarak became a national hero for his air defense prowess in the 1973 war against Israel?)

That leads to another possibility: “Just give people Thuraya satellite phones,” says John Pike of Globalsecurity.org. The cheapish phones hunt down signals from space hardware.

Even expanding access to the military’s own satellite communications networks is

US Has Secret Tools to Force Internet on Dictators

theoretically possible, Arquilla says. But he won't say more than that: "Let's just say that's an area decided at the level of the commander-in-chief."

In the absence of those options, there's always the old-school methods of jamming a government's communication frequencies and broadcasting favorable messages. That's the Commando Solo's specialty. "Jamming is something we think about in the context of shooting wars," says Arquilla, but "it may have its place in social revolutions as well."

The trouble is, if a government follows Egypt's lead and turns off the internet, it's not going to be keen to see a meddling foreign power turn it back on.

That act might not be as provocative as sending in ground troops or dropping bombs. But it's still an act of what you might call forced online entry — by definition, a hostile one.

In situations like Egypt, siding with an uprising against a longtime ally is a difficult choice, whether analog or digital.

That might be why the military hasn't done it. Asked about whether the Pentagon would consider deploying mobile connectivity to restore internet access for a social uprising, all a senior official would say is that such a situation was "hypothetical."

And all that underscores how Egypt's internet shutoff pushed the poorly defined limits of cyber hostilities. Foreign actors don't really have a blueprint for responding. The U.S. military "has a great deal of expertise on rebuilding communications network, but that's ... very different when the government is interested in resisting," Arquilla says. "This is far less an engineering problem and far more a political one."

The Cyberweapon That Could Take Down the Internet

The cyberweapon that could take down the internet

13:30 11 February 2011 by [Jacob Aron](#)

A new cyberweapon could take down the entire internet – and there's not much that current defences can do to stop it. So say [Max Schuchard](#) at the University of Minnesota in Minneapolis and his colleagues, the masterminds who have created the digital ordnance. But thankfully they have no intention of destroying the net just yet. Instead, they are suggesting improvements to its defences.

Schuchard's new attack pits the structure of the internet against itself. Hundreds of connection points in the net fall offline every minute, but we don't notice because the net routes around them. It can do this because the smaller networks that make up the internet, known as autonomous systems, communicate with each other through routers. When a communication path changes, nearby routers inform their neighbours through a system known as the border gateway protocol (BGP). These routers inform other neighbours in turn, eventually spreading knowledge of the new path throughout the internet.

A previously discovered method of attack, dubbed ZMW – after its three creators Zhang, Mao and Wang, researchers in the US who came up with their version four years ago – disrupts the connection between two routers by interfering with BGP to make it appear that the link is offline. Schuchard and colleagues worked out how to spread this disruption to the entire internet and simulated its effects.

Surgical strike

The attack requires a large botnet – a network of computers infected with software that allows them to be externally controlled: Schuchard reckons 250,000 such machines would be enough to take down the internet. Botnets are often used to perform distributed denial-of-service (DDoS)

The Cyberweapon That Could Take Down the Internet

attacks, which bring web servers down by overloading them with traffic, but this new line of attack is different.

"Normal DDoS is a hammer; this is more of a scalpel," says Schuchard. "If you cut in the wrong places then the attack won't work."

An attacker deploying the Schuchard cyberweapon would send traffic between computers in their botnet to build a map of the paths between them. Then they would identify a link common to many different paths and launch a ZMW attack to bring it down. Neighbouring routers would respond by sending out BGP updates to reroute traffic elsewhere. A short time later, the two sundered routers would reconnect and send out their own BGP updates, upon which attack traffic would start flowing in again, causing them to disconnect once more. This cycle would repeat, with the single breaking and reforming link sending out waves of BGP updates to every router on the internet. Eventually each router in the world would be receiving more updates than it could handle – after 20 minutes of attacking, a queue requiring 100 minutes of processing would have built up.

Clearly, that's a problem. "Routers under extreme computational load tend to do funny things," says Schuchard. With every router in the world preoccupied, natural routing outages wouldn't be fixed, and eventually the internet would be so full of holes that communication would become impossible. Shuchard thinks it would take days to recover.

"Once this attack got launched, it wouldn't be solved by technical means, but by network operators actually talking to each other," he says. Each autonomous system would have to be taken down and rebooted to clear the BGP backlog.

Meltdown not expected

The Cyberweapon That Could Take Down the Internet

So is internet meltdown now inevitable? Perhaps not. The attack is unlikely to be launched by malicious hackers, because mapping the network to find a target link is a highly technical task, and anyone with a large enough botnet is more likely to be [renting it out for a profit](#).

An alternative scenario would be the nuclear option in a full-blown cyberwar – the last resort in retaliation to other forms of cyberattack. A nation state could pull up the digital drawbridge by adjusting its BGP to disconnect from the internet, just as [Egypt did two weeks ago](#). An agent in another country could then launch the attack, bringing down the internet while preserving the attacking nation's internal network.

Sitting duck

Whoever launched the attack, there's little we could do about it. Schuchard's simulation shows that existing fail-safes built into BGP do little to protect against his attack – they weren't designed to. One solution is to send BGP updates via a separate network from other data, but this is impractical as it would essentially involve building a shadow internet.

Another is to alter the BGP system to assume that links never go down, but this change would have to be made by at least 10 per cent of all autonomous systems on the internet, according to the researchers' model, and would require network operators to monitor the health of connections in other ways. Schuchard says that convincing enough independent operators to make the change could be difficult.

"Nobody knows if it's possible to bring down the global internet routing system," says [Mark Handley](#), an expert in networked systems at University College London. He suggests that the attack could cause "significant disruption" to the internet, with an effect greater than the [Slammer worm of 2003](#), but it is unlikely to bring the whole thing down.

The Cyberweapon That Could Take Down the Internet

"The simulations in the paper make a lot of simplifying assumptions, which is necessary to simulate on this scale," he explains. "I doubt the internet would behave as described."

Schuchard and colleagues presented their findings at the [Network and Distributed System Security Symposium](#) in San Diego, California, on Tuesday.

Too Much Hysteria Over Cyber Attacks

Too much hysteria over cyber attacks: US experts

By Glenn Chapman (AFP) – 2 days ago

SAN FRANCISCO — Overblown talk of full-on cyber war between nations fueled by recent attacks like the computer worm Stuxnet could hamper Internet security efforts, officials and experts warned Tuesday.

Serious attention should be paid to threats of cyber attacks from hackers, spies and terrorist groups but not to the extent of mass hysteria, speakers at the premier RSA computer security conference in San Francisco said.

"Cyber war is a terrible metaphor," said White House cybersecurity czar Howard Schmidt. "Don't make it something it's not."

Online espionage and hacking are not new, and hyping incidents as warfare distracts computer security champions from critical jobs such as safeguarding power grids, financial systems, and medical networks, he contended.

"We are in the midst of a cyber war of words," Schmidt said. "Let's quit pointing fingers and start cleaning up the infrastructure."

Renowned computer security specialist Bruce Schneier of BT Group said that use of warlike tactics in online conflicts is fueling hysteria that has the world on the brink of a "cyber arms race."

"We are not necessarily seeing cyber war, but increasing use of warlike tactics in more general cyber conflicts," Schneier said. "I think that is what's confusing us."

He cited a Stuxnet computer virus evidently crafted to find and disrupt an Iranian nuclear facility as an Internet Age attack that smacks of warfare but arguably falls short.

"It is not war," Schneier said. "It is in the middle somewhere."

Fears of cyber war are driving a needless cyber arms race that brings with it the danger that software weapons might accidentally be released, he argued.

"We haven't seen offensive cyber weapons companies, but they are coming," Schneier said. "Big defense contractors are working on this; you know they would be dumb not to."

The most prevalent cyber threat has been theft of information from networks, US Deputy Secretary of Defense William Lynn said in a keynote address to the gathering. Foreign spy agencies have accessed military plans and weapons systems designs, while source codes and intellectual property have been swiped from businesses and universities, according to Lynn.

Too Much Hysteria Over Cyber Attacks

Attacks on computer networks have thus far been "relatively unsophisticated" and short in duration, the defense official said.

An emerging threat is that cyber tools will cause real-world damage, according to Lynn.

"The threat is moving up a ladder of escalation, from exploitation to disruption to destruction," he said.

Foreign spies have focused on mining US networks instead of disrupting them, according to Lynn.

"Although we cannot dismiss the threat of a rogue state lashing out, most nations have no more interest in conducting a destructive cyber attack against us than they do a conventional military attack," Lynn said.

"The risk for them is too great."

US defense officials are more worried about an accidental release of "toxic malware," he explained.

"Perhaps the greatest concern in our judgement is a terrorist group that gains the level of disruptive and destructive capability currently possessed by nation-states," Lynn said.

Terrorist groups could craft their own cyber weapons or buy them on the black market, he added.

"As you know better than I, a couple dozen talented programmers wearing flip-flops and drinking Red Bull can do a lot of damage," Lynn told the gathering of software savants.

"We have to assume that if they have the means to strike, they will do so."

Cyber commandos are being trained in the military, and the US is reaching out to allies to form collective online defenses, he said.

Lynn called on specialists in the computer security industry to team with the military to defend the nation's networks.

"The government cannot protect our nation alone," Lynn said. "It is going to take a public-private partnership to secure our networks."

Copyright © 2011 AFP. All rights reserved.

Navy Strengthens IT Capabilities Across Fleet

Navy Strengthens IT Capabilities Across Fleet

New approach to applications development will keep pace with innovations
(DEFENSE SYSTEMS 24 JAN 11) ... Barry Rosenberg

Rear Adm. Jerry Burroughs is the Navy's program executive officer for command, control, communications, computers and intelligence, a position he has held since March 2010. Burroughs previously was chief engineer at the Space and Naval Warfare Systems Command.

The Navy Program Executive Office for C4I acquires, fields and supports networks; communications; and intelligence, surveillance and reconnaissance systems for the Navy and Marine Corps, and it includes 10 Program Management Warfare (PMW) offices. Burroughs recently spoke to Defense Systems Editor-in-Chief Barry Rosenberg about the PEO's near-term priorities that involve technology upgrades, new development approaches and acquisition improvements.

DS: What's at the top of your to-do list right now?

Burroughs: We recently signed out our new strategic plan, which concentrates in three areas: minimizing costs, rapidly delivering new capabilities, and developing our workforce and equipping them to achieve acquisition excellence. Most importantly, we are laser focused on providing innovative and integrated capabilities that reduce total ownership costs, because in today's environment, cost has to be your first consideration.

DS: What are some of the cost targets you're aiming at?

Burroughs: I don't have an overall target for the PEO, but for every program that comes in, we set targets for what that program should cost and look for ways that we can reduce the costs. I don't know if you read [Undersecretary of Defense for Acquisition, Technology and Logistics] Ashton Carter's memo recently, but we are focused on what he said (regarding) the must or should cost [that gets technology to the field quicker]. The cost must be a key parameter that you look at as you go through all the milestones.

DS: Where within PEO C4I do you see an opportunity to reduce costs?

Burroughs: I think the biggest opportunity we have is reducing the number of programs we have. I have over 120 projects and programs, which is a tremendous amount to manage with the size of the workforce that I have. And a lot of them are legacy programs that take a lot of time and money in sustainment. And frankly, the older systems get, the more it costs to keep them going. So we have to get rid of the legacy systems and look for ways to transition to newer systems. If I could point to one thing and that will help us to reduce total ownership costs, that would be it.

DS: That is what the Navy has in mind with the Consolidated Afloat Networks and Enterprise Services (CANES) program, in which legacy systems will be replaced by commercial hardware that can be easily upgraded.

Burroughs: Absolutely. You know, we have networks out in the fleet now that are 10-plus years old. You can imagine that if you have a home computer that's 10 years old, it's not working very well, if by chance it's still working at all. And it's probably not very secure and takes a lot of your time to keep it going. So CANES is absolutely pivotal to the first two priorities that I mentioned earlier.

Navy Strengthens IT Capabilities Across Fleet

DS: What is PEO C4I doing to more rapidly deliver relevant capabilities to warfighters?

Burroughs: We have to look for more innovative ways within today's acquisition framework to get capability out to the fleet, but more importantly, you've heard a lot of talk about acquisition reform, especially in the IT arena. So as that evolves, I think that will offer us a lot of opportunities to more rapidly field capabilities.

DS: The topic of acquisition reform seems to come up every few years, as does the desire to rapidly field new capabilities. So what is it about the acquisition process now that prevents you from doing that? In other words, how do you speed the introduction of new technologies while dealing with the existing system?

Burroughs: Well, as you know, the existing system is very platform-focused, and it takes years to get through the requirements process, develop a design, and then field it. And that's probably appropriate for a ship or an airplane that has to last 35 to 40 years. But my systems are obsolete in five to six years in many cases. If you look at the way we did CANES, it's actually a pretty rapid program and is utilizing what was called the IT Box Acquisition Initiative. I don't know if you are familiar with that one.

DS: Tell me about it.

Burroughs: It was signed out last year as an initiative for IT systems that are software intensive and [commercial], and CANES luckily enough fit both of those, so we're taking advantage of that. IT Box is codified under [the Joint Capabilities Integration Development System]. While JCIDS can be quite cumbersome and at times appear to be overly bureaucratic, the IT Box was a fix/solution to accommodate the uniqueness and the frequency of technological innovations and capability/performance improvements associated with IT-related capability development. Additionally, [the Joint Staff's Force Structure, Resources and Assessment Directorate] just launched its communitywide effort to review JCIDS and develop recommendations to increase its responsiveness and decision support.

In addition, the Defense Science Board last year took a look at IT acquisition and came out with some recommendations that would condense the requirements process. It eliminates all the massive amounts of [Joint Requirements Oversight Council] oversight and implements a philosophy where you build a little, test a little, go back to the user and get some input from them, then go back into the lab, and develop a little more.

Most of the systems that we develop and build are really applications, frankly. With a few exceptions, most of our hardware will be limited to CANES. Everything else is just an application that we develop to write on CANES. So it is ideally suited to that and is where we are going in that area.

DS: What are the C4I technology enablers that are most important to the Navy and Marine Corps?

Burroughs: I would say first — and really most of these get back to what we are doing with CANES — is service-oriented architecture. It offers a great opportunity to more rapidly develop and fill applications. Next is virtualization, which is also a big enabler for the CANES construct and allows us to more efficiently utilize our hardware resources, if you will.

Navy Strengthens IT Capabilities Across Fleet

In addition, new visualization technologies are certainly key to where we're trying to go in the intelligence area, as well as developing a common operational picture.

DS: CANES is clearly your No. 1 program today. What would you say is No. 2 at PEO C4I right now?

Burroughs: Another one of our very important programs would be [the Navy Multiband Terminal]. And that is key as we talk about necking down systems. NMT replaces three or four legacy satellite terminal programs, so it's a new capability that we're rolling out. It's far superior to what we have out in the fleet today and is a win-win not only from a capability perspective but also from a total ownership cost perspective.

DS: What's the near-term road map for NMT?

Burroughs: It is just now going into [low-rate initial production]. We will be doing the testing over the next year or so and then full production after that.

DS: How many NMT units are being procured?

Burroughs: The Navy Multiband Terminal will be fielded on 276 ships.

DS: What's new with the Navy's primary command and control system, the Global Command and Control System-Maritime (GCCS-M) program?

Burroughs: We are continuing to build capabilities into that, and we will morph it into an application that will ride on CANES. The key there will be a more streamlined system that better integrates with CANES and provides not only more capability but also a better user experience and more robust reliability. Further down the line, we'll go into the Maritime Tactical Command and Control System, which we see as a follow-on to GCCS.

DS: We have talked a lot about the C4 aspect of PEO C4I but not much about the intelligence aspect. How do you view the connective between C4 and I?

Burroughs: Well, I'll put it this way. I don't know if you've read a lot of the precepts related to information dominance that have come out of the N2N6, [the Navy's offices for intelligence and information technology]. One of their precepts is that every ship is a sensor, and every sensor is a node. So if you think of it that way, it's absolutely critical how you link those ships and nodes together. And intelligence is just information that we're passing between those nodes with some analysis that goes on top of it. So C4 and intelligence really go hand in hand because intelligence absolutely depends on the ability to rapidly move the right information to the right places.

DS: You recently created a new office, the Information Assurance and Cyber Security Office. Can you tell me what that's all about? What prompted it? What do you expect it to do?

Burroughs: Yes, PMW130 was in response to the Defense Department standing up the Cyber Command and the Navy, in turn, standing up the 10th Fleet in January 2010. So in line with that, we needed to have a greater focus on cyber, security and cryptographic systems. That had traditionally fallen in with our networks program, which was part of PMW160. To give that greater focus and to have a program manager who is directly responsible for those areas, we decided that standing up PMW130 was the right way to go.**DS:** What specifically might PMW130 do that was not done when they were part of one of the other PMW offices?

Burroughs: I wouldn't say that there is anything that they're specifically doing that they

Navy Strengthens IT Capabilities Across Fleet

weren't doing before, but you now have a program manager and a deputy program manager who are solely responsible for that and who are solely concentrating in those areas.

Actionable Intelligence

Actionable Intelligence

As data pours in, Navy officials must decide how best to use it

(SEA POWER MAGAZINE FEBRUARY 2011) ... Daniel P. Taylor

The proliferation of sensor-laden drones, the advancement of intelligence, surveillance and reconnaissance technology, and the development of networks for virtually every platform during the last decade has left the Navy with a unique problem: How does it make this massive inflow of data useful?

“Our problem generally isn’t getting information,” said Terry Halvorsen, Navy chief information officer. “As a matter of fact, I would argue that, many times, we have almost too much information.”

When data and information come pouring in from all sorts of sensors in the field, the challenge is to turn it into something that can be used on the battlefield or in planning Navy strategy, Halvorsen said, which is why the service is placing a special focus on what is known as network-centric warfare.

“How do you take all that information and data and turn it into actionable intelligence — data that’s meaningful and relevant to a decision-maker?” Halvorsen said.

Turning Navy platforms, regardless of type, into net-centric systems is a difficult task. First of all, not all data is urgently needed in the field.

“If you’re [engaged in] a strategic effort, you’ve got a little more time to get the data,” Halvorsen said. “If you’re in a tactical engagement, you need the data then, so you need a way to get data to the right commander in time for it to influence his tactical battlefield decision.

“That’s really what net-centricity is about,” he said. “The commander that has the best data, at the time he needs it, generally wins.”

For Capt. Brian Pearson, networks branch head at the newly minted N2/N6 “information dominance” directorate, the term “information dominance” is “about getting the information to the commander, allowing the commander to figure out what he needs.”

Capt. Jack Steiner, tactical and strategic communications branch head at N2/N6, said it’s about giving commanders the right data at the right time so they can adapt to the situation at hand.

“The initial discussions in all this were about the ability of the force to synchronize and self-synchronize ... [and] making the flow of information more ubiquitous and available,” he said. “That way, content isn’t sitting in an airframe and waiting to get back and land. As soon as information is available, we’re transmitting the information.”

Actionable Intelligence

Right now, commanders are constrained by the fact that they often have to manually process data from wherever they get it. There may be a critical piece of data out there that could help, and the commander would never know about it.

For example, Steiner said that 10 years ago in the Persian Gulf, when the Navy did mining, someone would find the mine and then write a message that included the coordinates and broadcast it to certain people, but there was no common picture from which everyone could draw information. Today, mine-countermeasures ships can draw information from sensors and feed it into a picture that can be distributed to the force, something that needs to happen across the fleet in all areas, he said.

“It’s less about enabling commanders to do something they’re not doing,” Pierce added. “It’s more about enabling the information a commander needs to get there as soon as it can get there.”

What makes that goal even more challenging is the fact that technology is constantly evolving, and so is the threat. While Halvorsen feels the Navy is where it needs to be “given what I know today,” the challenge for the service is “building in the agility to be able to change any component if the environment changes.”

The challenge is not about technology or resources, but “are our processes agile enough?” Halvorsen said.

He noted the key to having a truly network-centric force that can quickly process data and use it to counter the threat immediately is being able to filter the information, determine who needs it and when, and be able to adjust to any scenario. And it applies not just to the tactical environment. The Navy must be able to switch gears when it comes to budgeting and acquisition when new information about threats in the field comes to light.

“I would say it’s the thing I spend the most time thinking about,” Halvorsen said. “How do we keep up with the agility required? Are we agile enough to change what we thought we needed to buy in acquisition?”

Security is another issue when it comes to net-centricity, he said. Some data needs a heavy amount of security and encryption, but other data — such as information on the movements of a nearby enemy that goes to a combat patrol — is quickly dated and useless to an enemy so it does not need to be as secure. Adding security in those situations is counterproductive, Halvorsen said.

“When you add security ... many times you are impacting the speed of transition,” he said. “That’s what we’re consistently looking at: closing the gap between combat systems and C4I [command, control, communications, computers and intelligence] systems.”

Another Navy goal for net-centricity is consolidating the myriad networks currently on ships and land into one network, such as the Consolidate Afloat Network and Enterprise Services currently being developed that will combine legacy networks aboard ships into one modern

Actionable Intelligence

network. Its land-based counterpart is the Next-Generation Enterprise Network, which also is under development and will replace the Navy-Marine Corps Intranet in the coming years.

The Navy also is seeking to consolidate the programs themselves. In summer 2009, the Navy merged the intelligence (N2) and communications (N6) directorates in the Office of the Chief of Naval Operations and created N2/N6. The service transferred surveillance assets such as unmanned aerial systems to the new directorate. The merger was a key event in the evolution to a net-centric Navy, Halvorsen said.

“It’s the linking of intelligence and communications,” he said. “It puts all the information tenets into at least one group.”

No individual platform is central to the push for net-centricity, Pierce said.

“Every platform has the ability to collect information depending on its characteristics,” he said. “There’s a lot of focus these days on these new platforms and getting more and more sensors out there gathering data. Our challenge as network and communications folks is to make sure leadership knows that you can gather all the data you want, but until you get it back to where it can be processed and disseminated, you just have a lot of data out there.”

The challenge for the Navy and industry in the future will be to develop systems and networks that can filter out the relevant information and send it to the appropriate people at the right time. But another key part of getting net-centricity to work in the Navy is changing how combatant commanders think, although Halvorsen declined to refer to it as “changing the culture.”

“When I have a defined set of data, I’m much more comfortable with that — here’s the data I’ve got to look at to get an answer,” he said. “Net-centricity says you’ve got to look at a broader set of data, so you have to train and educate people to look at a broader set of data, particularly in the network world.

“You can’t let a physical or geographic focus be your driver,” he continued. “That’s probably the single biggest change in the network world you’ve got to think about. Now you’ve got to get a commander to think what it means to command his piece of cyberspace. He’s got to understand that a network event totally outside of his geographic region can have a big impact on him.

“Culture might not be the right word,” he added. “It’s more of a warfighting mindset.”

US Military Says Keeps Up With China; Is it enough?

Analysis: U.S. military says keeps up with China; Is it enough?



By Phil Stewart

WASHINGTON | Tue Feb 1, 2011 1:11am EST

(Reuters) - U.S. military commanders are expressing confidence that they can hold their own in the face of faster-than-expected advances by China's military, but looming

US Military Says Keeps Up With China; Is it enough?

cost cuts are adding to doubts about the future of American power in the Pacific.

Fueled by its booming economy, China's military growth over the past decade has exceeded most U.S. forecasts. Its plans to develop aircraft carriers, anti-satellite missiles and other advanced systems have alarmed neighbors and Washington.

Critics, including within the U.S. Congress, note with apprehension that rising Chinese defense spending coincides with Washington's plans to scale back its budgets.

They accuse the Pentagon of appearing flat-footed in its response to China's military advances, like the development of a stealth fighter jet and a new missile that could challenge U.S. aircraft carriers.

"I think we're headed on the wrong track," Randy Forbes, a Republican lawmaker who is part of the Congressional China Caucus, told Reuters.

Experts agree that as China's military expands its reach, the risks of potentially dangerous misunderstandings between the U.S. and Chinese armed forces will increase.

But they are divided over whether China's rise necessarily means a decline in power for the U.S. military, or whether it can indefinitely preserve its edge through investments, technological advances and strengthened Asian alliances.

Moreover interdependence between the world's two largest economies creates little incentive for conflict, but regional frictions may ultimately prove the most likely spark for confrontation, experts say.

The debate over whether the United States can preserve its military advantage hits home for the U.S. Navy, which is tasked with preserving U.S. access to international waters around China that the People's Liberation Army appears intent on controlling.

US Military Says Keeps Up With China; Is it enough?

In an interview from an office at the Washington Navy Yard, a military base in the nation's capital, the top Navy commander said the military had plans in place to cope with advances in China, and elsewhere. "We're not flat footed" in the response to China, Admiral Gary Roughead told Reuters.

"I would say that we are responding, or advancing, our capabilities in such a way that we're pacing the global developments that are taking place," he said.

"That includes Chinese advances, it includes developments that are taking place in other parts of the world as well."

U.S. Defense Secretary Robert Gates added his voice to such assurances, saying the United States needed to "respond appropriately with our own programs" to Chinese advances.

Some analysts warn that the United States cannot hedge against every future Chinese capability in an era of tight spending. Then there are practical limitations of providing security in Asia.

"The problem is that for China, it's a home game. For us, it's an away game," said James Carafano, a defense analyst at the Heritage Foundation, a conservative think-tank.

"We've got this razor thin margin (of error) and they're assuming (at the Pentagon) they have perfect knowledge and know exactly what the Chinese are going to do."

ARE FEARS OVERBLOWN?

The core U.S. defense budget -- not including war funding -- was \$530 billion in 2010. That's well beyond China's 532.1 billion yuan (about \$80 billion) in official defense spending. Analysts believe that China's military spending is much higher than it

US Military Says Keeps Up With China; Is it enough?

publicly admits.

"The Chinese are not 10 feet tall," said Admiral Mike Mullen, who as chairman of the U.S. military's Joint Chiefs of Staff is the top U.S. military officer.

A top Chinese official acknowledged recently the United States will retain unchallengeable global dominance for at least two decades.

Still, analysts point out that Chinese advances in areas like cyber warfare could more quickly level the playing field. The U.S. military can invest heavily in new capabilities, but it will always have weaknesses that can be exploited.

A U.S. military official, speaking on condition of anonymity, said exercises and simulations conducted by the U.S. military have taken into account new technologies and capabilities in the region that could alter the status quo. The official declined to cite China specifically.

Pentagon officials, when asked about China, have pointed to a five-year budget plan that -- while lower than initially projected -- still invests heavily in new technologies like a new generation of long-range nuclear bombers, jammers and radar.

The U.S. military does not expect to build new bases in Asia in the near future but aims to "enhance" its presence in Southeast Asia while maintaining it in Northeast Asia, Gates said recently.

There are nearly 80,000 U.S. military personnel stationed in [Japan](#) and South Korea alone. Gates recently warned an audience in Tokyo that China "might behave more assertively toward its neighbors" without the U.S. presence in Japan.

INEVITABLE ADVERSARIES?

Gates, for one, has said he did not believe the United States and China are "inevitable

US Military Says Keeps Up With China; Is it enough?

strategic adversaries."

The United States and China are the world's two largest economies, and some analysts say their economic dependency and shared interest in global stability will over time smooth tensions -- and lower the risk of conflict.

"The Chinese do not want to go to war with us. They own too much of our debt, and rely too much on us for trade," said Chris Hellman of the nonprofit National Priorities Project.

But whether China's economic growth translates into better military relations remains an open question, particularly if Pentagon officials are correct in saying Beijing is developing arms specifically designed to counter U.S. capabilities.

China's navy has alarmed neighbors with aggressive behavior, and last year's flare-up of a territorial dispute over islands -- known as Senkaku in Japan and Diaoyu in China -- set off alarms in the region.

"Are we heading toward a clash between the U.S. and China? I don't think so," U.S. Vice Admiral David Dorsett, director of naval intelligence, said in January.

"I would be more worried about an inadvertent tension, crisis, conflict over the Senkakus with the deployment of Chinese maritime-associated ships," he said.

(Additional reporting by [Andrea Shalal-Esa](#); Editing by [Cynthia Osterman](#))

Air Force Grapples with Bandwidth and Workforce Shortages

Air Force grapples with bandwidth and workforce shortages

February 7, 2011 — 12:54pm ET | By [Molly Bernhart Walker](#)

Senior Air Force officials say the service branch will soon face bandwidth shortages. As new surveillance technology deploys in combat zones, bandwidth needs are increasing exponentially, said Randy Walden, director of Information Dominance, SAF/AQI during a Feb. 4 [AFCEA DC](#) event in Arlington, Va.

"There's been conversations of, 'If you liked full-motion video, you're going to love Gorgon Stare.' And then you're going to absolutely require that we get more area, more persistence and better resolution which, guess what, drives that bandwidth even further," said Walden.

Bandwidth considerations are a key component of coming information technology procurements, he said.

Workforce bandwidth is a growing concern for Air Force as well, said Steve Wert, program executive officer C4ISR, Electronic Systems Center, Hanscom Air Force Base.

"The atrophy that happened, especially in our government workforce, really is shocking. We went so far below critical mass," he said.

Upon becoming PEO, Wert reviewed projects that only had "a handful" of employees managing a billion-dollar program. "We clearly went too far," he said, referring to cuts in C4ISR acquisition staff.

As Air Force addresses acquisition staffing and program management, Wert said he does see some promising trends. Service-oriented architecture is becoming more readily available and offerings are more competitive, he said.

Air Force is also making gains in agile development adoption, said Wert, and all the programs he oversees have 12-month, or less, development cycles and 18 months to the field. Big, multi-year development programs for the IT domain are just "flat out inappropriate and wasteful," said Wert.

Wert also said there needs to be greater accountability for program execution. "Cost and schedule overruns are really such commonplace occurrences and how we do business that we kind of become used to it. That represents a huge waste in

Air Force Grapples with Bandwidth and Workforce Shortages

resources," said Wert. "We really need to focus on that."

Wert added that the DoD 5000 gives acquisition managers the flexibility and agility it needs for successful execution. "The DoD 5000 actually gives the milestone decision authority the authority to waive everything other than statute, including DoD 5000. We actually have, under this structure, the ability to do business the way that we think is most appropriate."

Cybersecurity Runs Deep in Fiscal 2012 Budget Request

Cybersecurity runs deep in fiscal 2012 budget request

February 16, 2011 — 10:37am ET | By [David Perera](#)

Cybersecurity gets robust attention in the fiscal 2012 budget request released Feb. 14 by President Obama, with federal agencies requesting billions of dollars dedicated to cyber.

The Homeland Security Department wants \$936.48 million for "infrastructure protection and information security," considerably more than the \$836 million it got for that line item in fiscal 2010, but less than the \$1.07 billion it's projected to spend during the current fiscal year. This line item funds, among other activities, the National Cyber Security Division, the National Communications System and the Office of Emergency Communications.

The majority of the nearly \$1 billion request would go toward cybersecurity and emergency communication efforts, according to detailed information contained in the department's congressional budget justification [document](#) (.pdf)

Specifically, nearly \$614.21 million, or about 66 percent of the line item, would go toward cybersecurity and communications. Einstein, the governmentwide network intrusion detection system spearheaded by DHS, would receive a \$233.6 million chunk of that money (38 percent), likewise a marked increase over years past. In fiscal 2010, Einstein received \$193.67 million, and DHS is projected to spend that much on it this year.

Already in the current fiscal year, DHS plans to initiate procurement and commence development of EINSTEIN 3 capabilities in partnership with the National Security Agency, the justification document says. The end of fiscal 2012 should see deployment of the first set of five Einstein 3 sensors and five of the 15 "nests" (Internet traffic aggregation points) the security program intends to have fully operational in fiscal 2016, the document adds.

"This deployment will represent the first enablement of active defense capability to prevent and/or limit malicious activities from penetrating the .gov environment," it states.

The National Institute of Standards and Technology requests \$678.94 million to be available until expended for scientific and technical research and services, a notable increase in new budget authority from the \$515 million Congress gave NIST in fiscal

Cybersecurity Runs Deep in Fiscal 2012 Budget Request

2010 and the \$515 million the agency is projected to spend this year.

Part of that bump is due to NIST's cybersecurity program (what NIST is calling "Ensuring a Secure and Robust Cyber Infrastructure") which would receive a \$43.3 million increase. \$24.5 million of that would go to the [National Strategy for Trusted Identities in Cyberspace](#), while the [National Initiative for Cybersecurity Education](#) would get \$4 million. A new effort also called the Scalable Cybersecurity for Emerging Technologies and Threats would get \$14.9 million.

The Defense Department, meanwhile, wants to spend \$2.3 billion on improving its cyber capabilities.

Included in that amount is \$500 million over five years for the construction and equipping of a Joint Operations Center for Cyber Command at Ft. Meade.

The Defense Advanced Research Projects Agency would also get \$500 million to invest in cyber technologies.

According to DARPA budget justification material, DARPA would spend \$10 million on the Comprehensive National Cybersecurity Initiative, a 12 point multiagency program started in January 2008. The \$10 million would fund a national cyber range for testing software in a simulated Internet. The requested amount is less than the \$49.79 million DARPA spent on the CNCI in fiscal 2010 and the \$10 million it's projected to spend this fiscal year.

The research agency would also continue to fund an effort known as Cyber Genome, increasing its fiscal 2012 budget to \$24 million, more than the \$8.5 million the program received in fiscal 2010 and the 413 million it's projected to receive this year. Cyber Genome is meant to develop "breakthrough cyber-forensic techniques to characterize, analyze, and identify malicious code" allowing for the automatic detection of even previously unknown malicious code.

DARPA would also fund new cyber programs, including \$6.5 million to develop "crowd-sourced approaches for verifying the correctness of software systems" in an effort called, straightforwardly, Crowd-Sourced Cyber.

It would also give \$4.67 million for Cross-Layer Network Security, a program that would develop "novel approaches for enhanced network security that involve multiple networked layers" that has the potential of defeating distributed denial of service attacks, at least in wireless networks. DARPA contrasts this potential new approach

Cybersecurity Runs Deep in Fiscal 2012 Budget Request

with typical standard Internet protocol security implemented in just the network layer. A cross layer approach in a wireless network could use emerging path diversity technologies to introduce route diversity as a cybersecurity mechanism, the budget justification says.

A new Cyber Reserve Corps program would get \$20 million under the request. The effort would "develop technologies and tools to enable and educate private citizens to participate in the defense of cyberspace."

A likewise new effort called Resilient Networks would also get \$20 million to develop routing/switching software for commodity processors for use in responding to cyber attacks. "Such software-defined routers/switches will enable far greater agility in responding to exploits than is presently possible and provide the basis for highly reactive networked defense capabilities," the DARPA budget justification document states.

DARPA also wants \$15.83 million start a program for a cybersecurity program that would allow systems to "mimic camouflage concealment, and deception in the physical world." The effort, Cyber Camouflage, Concealment and Deception, would look to create a way for network resources such as switches, servers and storage to be virtually replicated to confound enemy targeting.

Hacker Peiter "Mudge" Zatkoff's effort to detect inside threats by identifying certain system and network activities would gain \$12 million for another year of funding. The program, Cyber Inside Threat, aka [CINDER](#), received \$5 million in fiscal 2010 and is projected to spend \$10.5 million this fiscal year.

For more:

- download .pdfs of the DHS [fiscal 2012 budget in brief](#), or the [congressional budget justification](#), or a [fact sheet](#)
- [go to](#) a NIST webpage on its fiscal 2012 budget request
- [go to](#) a DoD webpage with links to its fiscal 2012 budget request material
- [download](#) DARPA's fiscal 2012 budget justification (.pdf)

The Inside Story of How Facebook Responded to Tunisian Hacks

The Inside Story of How Facebook Responded to Tunisian Hacks

JAN 24 2011, 1:20 AM ET

By

ALEXIS MADRIGAL

It was on Christmas Day that Facebook's Chief Security Officer Joe Sullivan first noticed strange things going on in Tunisia. Reports started to trickle in that political-protest pages were being hacked. "We were getting anecdotal reports saying, 'It looks like someone logged into my account and deleted it,'" Sullivan said.

For Tunisians, it was another run-in with Ammar, the nickname they've given to the authorities that censor the country's Internet. They'd come to expect it.

In the days after the holiday, Sullivan's security team started to take a closer look at the data, but it wasn't entirely clear what was happening. In the US, they could look to see if different IP addresses, which identify particular nodes on the network, were accessing the same account. But in Tunisia, the addresses are commonly reassigned. The evidence that accounts were being hacked remained anecdotal. Facebook's security team couldn't prove something was wrong in the data. It wasn't until after the new year that the shocking truth emerged:

Ammar was in the process of stealing an entire country's worth of passwords.

* * *

Here's what's at stake. December of 2010 saw the most substantial civil unrest in Tunisia in the reign of Zine El Abidine Ben Ali, which began with a bloodless coup in November 1987. Beginning with street protests in the country's poor interior region of Sidi Bouzid, the calls for change were soon echoed by more powerful civil society organizations, notably the country's only labor union, the UGTT. But despite the turmoil, it wasn't clear what exactly might happen.

"It is too early to know if these protests signal the beginning of the end for Ben Ali,"

The Inside Story of How Facebook Responded to Tunisian Hacks

wrote [Christopher Alexander in *Foreign Policy* on January 3](#). "However, Tunisia's current political scene looks a bit like it did in 1975 and 1976, the beginning of the long slide for Ben Ali's predecessor, Habib Bourguiba."

That is to say, even expert analysts of the country couldn't tell if Ben Ali would remain in power for a few more weeks or a decade. It did not feel inevitable that Ben Ali would be deposed. People had protested in the streets before. Revolution had been in the air. It wasn't clear that this time would be different.

There has been a lot of debate about whether Twitter helped unleash the massive changes that led Ben Ali to leave office on January 14, but Facebook appears to have played a more important role in spreading dissent.

"I think Facebook played a bigger role in this case," said Jillian York of the Berkman Center for the Internet and Society, who has been tracking the Tunisian situation closely. "There are a lot more Facebook users than Twitter users. Facebook allows for strong ties in a way that Twitter doesn't. You're not just conversing."

One early sign that Tunisians felt Facebook could be useful: Back in July, bloggers [Photoshopped a picture of Mark Zuckerberg](#) to show him holding up a sign that read, "Sayeb Sala7, ya 3ammar," the slogan for a freedom of expression campaign late in 2010. Later, Zuckerberg popped up on [a sign outside the Saudi Arabian embassy](#) carried by Tunisian protesters demanding the arrest of Ben Ali.

The Inside Story of How Facebook Responded to Tunisian Hacks



York said that Tunisian bloggers and activists had told her that the ability to upload video to Facebook drove its usage because many other video-sharing sites had been blocked by the government.

The videos -- shot shakily with cameraphones -- created a link between what was happening on the streets in the poor areas of the country and the broader Tunisian population. Many are graphic. In one video -- since taken down, apparently -- a young man is lying on a gurney with his skull cracked open. Brain oozes out. Cries are heard all around. The video focuses in on the man's face and as the camera pulls back, we see that there are two other people with cameraphones recording the injury. Video after video of the revolutionary events captures other people videoing the same event. Those videos, and the actions they recorded, became the raw material for a much greater online apparatus that could amplify each injury, death, and protest.

But it wasn't just videos that people were sharing. All kinds of information passed between Tunisians. For activists as well as everyday people, Facebook became an indispensable resource for tracking the minute-by-minute development of the situation. By January 8, Facebook says that it had several hundred thousand more users than it had ever had before in Tunisia, a country with a few more people than Michigan. Scaled up to the size of the U.S., the burst of activity was like adding 10 million users in a week.

The Inside Story of How Facebook Responded to Tunisian Hacks

And the average time spent on the site more than doubled what it had been before.

Rim Abida, a Tunisian-born, Harvard-educated development consultant now living in Rio de Janeiro, said that over the course of the events, her "relationship to Facebook changed entirely."

"It basically went from being a waste of time or procrastination tool, to my go-to source on up-to-date information," Abida wrote in a Facebook message to me. "My mom is back in Tunisia on her own, and my Tunisian network on Facebook was posting the most up-to-date info on what was happening on the ground. It was stuff the major media channels weren't reporting, such as numbers to call to reach the military and what was happening when in what specific neighborhood."

In between the scenes of local unrest and people like Abida, there was a whole stratum of bloggers, writers, and social media sharers who watched and shared important videos.

While clashes with security forces took place in the streets, Rim, who asked we not use her last name, was in her bed in her apartment in Tunis. Like the blogger cliché, Rim sat in her pajamas sharing videos. In her hands, small protests that reached 50 people could suddenly reach another 50, who would share it with another 50. The idea that it might be time for the regime to change spread from city to city faster than street protests and even middle class places got involved.

Rim doesn't think the Tunisian revolution was a "Facebook revolution," but it was sufficiently important that when rumors started to fly on the 13th about what kind of retaliation the government was prepared to take, it took this form:

"There were rumors that Facebook or electricity was going to be shut down," Rim IM'd me from Tunis. "Or both."

* * *

After more than ten days of intensive investigation and study, Facebook's security team

The Inside Story of How Facebook Responded to Tunisian Hacks

realized something very, very bad was going on. The country's Internet service providers were running a malicious piece of code that was recording users' login information when they went to sites like Facebook.

By January 5, it was clear that an entire country's worth of passwords were in the process of being stolen right in the midst of the greatest political upheaval in two decades. Sullivan and his team decided they needed a country-level solution -- and fast.

Though Sullivan said Facebook has encountered a wide variety of security problems and been involved in various political situations, they'd never seen anything like what was happening in Tunisia.

"We've had to deal with ISPs in the past who have tried to filter or block our site," Sullivan said. "In this case, we were confronted by ISPs that were doing something unprecedented in that they were being very active in their attempts to intercept user information."

If you need a parable for the potential and pitfalls of a social-media enabled revolution, this is it: the very tool that people are using for their activism becomes the very means by which their identities could be compromised. When the details are filled in on the abstractions of Clay Shirky and Evgeny Morozov's work on the promise (former) and danger (latter) of Internet activism, the ground truth seems to be that both had their visions play out simultaneously.

At Facebook, Sullivan's team decided to take an apolitical approach to the problem. This was simply a hack that required a technical response. "At its core, from our standpoint, it's a security issue around passwords and making sure that we protect the integrity of passwords and accounts," he said. "It was very much a black and white security issue and less of a political issue."

The software was basically a country-level keystroke logger, with the passwords presumably being fed from the ISPs to the Ben Ali regime. As a user, you just logged into some part of the cloud, Facebook or your email, say, and it snatched up that information. If you stayed persistently logged in, you were safe. It was those who logged

The Inside Story of How Facebook Responded to Tunisian Hacks

out and came back that were open to the attack.

Sullivan's team rapidly coded a two-step response to the problem. First, all Tunisian requests for Facebook were routed to an https server. The Https protocol encrypts the information you send across it, so it's not susceptible to the keylogging strategy employed by the Tunisian ISPs.

The second technical solution they implemented was a "roadblock" for anyone who had logged out and then back in during the time when the malicious code was running. Like Facebook's version of a "mother's maiden name" question to get access to your old password, it asks you to identify your friends in photos to complete an account login.

They rolled out the new solutions to 100% of Tunisia by Monday morning, five days after they'd realized what was happening. It wasn't a totally perfect solution. Most specifically, ISPs can force a downgrade of https to http, but Sullivan said that Facebook had not seen that happen.

Though Sullivan is the unflappable type, the Tunisian situation seemed to force him into a bit of reflection. "When you step back and think about how Internet traffic is routed around the world, an astonishing amount is susceptible to government access," he noted.

And if governments around the world can, at least hypothetically, compromise users, it makes you wonder, [as the Berkman Center's Jillian York has](#), why Facebook hasn't implemented special tools or processes for activists. The biggest issue is that political dissidents often do not want to use their real names in places where activism can get you killed. Facebook has adamantly opposed activists attempts to use pseudonyms.

"We get requests all the time in a few different contexts where people would like to impersonate someone else. Police wanting to go undercover or human rights activists, say," Sullivan said. "And we, just based on our core mission and core product, don't want to allow that. That's just not what Facebook is. Facebook is a place where people connect with real people in their lives using their real identities."

Does Facebook have to go the extra mile to support activists? Sullivan said that

The Inside Story of How Facebook Responded to Tunisian Hacks

preliminary work has been done to create a special complaint reporting process for NGOs and other activists, a move that would address one long-time complaint.

More generally, though, Facebook certainly don't seem to be under any obligations to provide special treatment. But if Facebook really *is* becoming the public sphere -- and wants to remain central to people's real sociopolitically embedded lives -- maybe they're going to have to think beyond the situational technical fix. Facebook needs to own its position as a part of The Way the World Works and provide protections for political speech and actors.

Because the protests and overthrow of Ben Ali were just the beginning of this story. Hopes are high, but as we've seen so many times in the global south, the exit of one corrupt dictator usually means the entrance of another. To avoid that fate, politically active Tunisians will be using all of the tools at their disposal, including and maybe especially, Facebook. In fact, Rim said, it's already being used to debate how to create a new government and a better Tunisia.

There's No Such Thing as 'Social Media Revolution'

There's no such thing as 'social media revolution'

by [Caroline McCarthy](#)

There seems to be a contingent out there that analyzes each of the globe's various political conflicts and attempts to figure out, through plenty of speculation and the occasional Wikipedia look-ups of far-flung sovereignties, which uprising will mark the first true "social media revolution."

A dictator toppled by Twitter or ousted through the efforts of a Facebook group? It's an enticing idea, particularly for those who are in the business of social media and have a personal stake of sorts in tallying each instance of social media's global value making headlines. Twitter punditry this week has been peppered with speculation about whether upheaval in Tunisia or the subsequent [anti-government protests in Egypt](#) might amount to the "first" true revolution spawned by social media. But this just isn't the right way to measure things: the occurrence of a "social media revolution," at this point, should be neither noteworthy nor remarkable. If a dictator is overthrown or a government ousted, it would be notable if Facebook or Twitter *weren't* used.

That's because social media is a part of the world we live in and has become such a crucial form of communication that it will factor into any political movement nearly anywhere in the world. In other words, the use of Twitter, Facebook, or YouTube should not be what's worth talking about. At this point, it takes away from the substance of the revolution (or lack thereof) itself.

This sort of rhetoric has been going on for nearly two years when [an anti-government uprising in Iran](#) swelled up through Twitter and, as a result of traditional media crackdowns, became the primary medium in which much of the world knew about what was going on in the Islamic nation. The activists' efforts ultimately had far less impact on the government than many of the breathless Twitter observers expected, and for too many of them it's now known as the movement in which everyone tinted their Twitter profile photos with green as a sign of solidarity (which now seems awfully passive). This, alas, wasn't "the social media revolution." And so the pundits moved on.

So let's look at the basic numbers. Facebook has more than 600 million users around the world, an inarguable lock on the mainstream in much of the world and significant penetration even in the countries where it doesn't have as much reach. Twitter is about one-third its size, though its most active users tend to be more in the vein of newshounds and culture fans than FarmVille players and vacation photo swappers--which may be the reason why the smaller Twitter is as important, if not more so, than Facebook in political activism. Both social media services are actively looking to expand their reach in developing countries, particularly Facebook, which has launched mobile sites and applications [geared to lower-end cell phones and slower connections](#).

The truth is that smaller elements of "social media revolution" have been all around us already for over half a decade--even in our own, comparatively humdrum political system in which "revolution" means a switch in the partisan balance of a governing body accompanied by plenty of red-and-blue news-ticker graphics on cable networks. George Allen, a Republican senator from Virginia, was in a tight race for win re-election in 2006 until [a video from a campaign rally](#)

There's No Such Thing as 'Social Media Revolution'

surfaced on YouTube in which he called one of his opponent's campaign staff volunteers by a bizarre epithet that turned out to be a racial slur of sorts. The video went viral, Allen lost, and his "macaca moment" has been widely highlighted as the source of his downfall--in spite of the presence of countless strategists, publicists, and glossy campaign ads, social media's power prevailed.

Yes, social media can lead to the improbable rise of leaders who otherwise might never have had a shot. Without Meetup and the readership of liberal blogs, former Vermont governor Howard Dean might never had had a shot at the Democratic presidential nomination (which, of course, he lost). In 2008, Barack Obama's campaign team's digital savviness was a crucial component in the candidate's popularity among young voters who heavily favored him at the polls. Two years after Obama's inauguration, these things should no longer surprise us--nor should be we be surprised that, yes, social media is a vital instrument in political change all over the world.

That's the way things are in an age full of widely accessible yet largely uncontrolled media, in which the barrier to entry for any individual has been vastly lowered and the potential power of an organized mass can impact longstanding establishments. These technological developments have been groundbreaking. But they are not new. And "revolutionaries," whoever they may be, will use social media as an expanded set of tools for the tasks that have always been and remain the most crucial to activists: amassing support, communicating with like-minded people, and spreading the word. The tactics haven't changed. It's just that the available channels of communication have expanded.

Where it does get interesting, social media-wise, is where and when governments choose to crack down. On Tuesday evening, Twitter finally confirmed that Egypt was blocking access to its service after initially refusing to comment on the matter directly, but there were no reports on attempts to control Facebook or any other grassroots organization tool. This sort of thing provides some insight into what a government sees as its biggest digital threats and how it attempts to control and dissuade opposition forces. But the real focus ought to be on what's being said. The real meat of a political uprising is the message itself, and hype about digital media's impact on it all should be well enough accepted by now that it shouldn't take over the limelight.

And, should that successful "social media revolution" come along, I hope the digerati gives the successful activists some credit: If they topple a dictator, the real reason isn't that Facebook Groups made it possible for them to organize or because they generated a clever Twitter hashtag. Social media has changed the world, but by no means does it provide a substitute for the human energy and willpower that can bring down governments and cause global reverberations. Let's focus on understanding what really happens.

Besides, if you're keeping a scorecard for social media, you might want to note that, 600 million Facebook users later, it's already won.

Social Media Revolution Hits Saudi Arabia

Social Media Revolution Hits Saudi Arabia

by DEBORAH AMOS



Fahd Shadeed/AFP/Getty Images

Ahmed al-Omran, a 22-year-old Saudi university student, checks his Internet blog on his laptop computer at a cafe in Riyadh, Saudi Arabia, on June 5, 2006.

January 26, 2011

There is a social media revolution in Saudi Arabia.

Ten million Saudis are online, 3 million belong to Facebook, and Twitter feeds are up more than 400 percent.

Recently, many tweets and posts have been focused on the uprising in Tunisia. In fact, Saudi's social media activists spread videos and news updates at the peak of the street protests — and the interest has stayed high ever since. And, now, Saudi bloggers have added the unrest in Cairo to the topics receiving much attention.

What Now?

Will the Saudi government clamp down on this free-wheeling speech after Tunisia's social media movement helped to bring down a government?

Social Media Revolution Hits Saudi Arabia

It's one of the big questions ahead for Saudi Arabia. How this authoritarian regime will live with the freedom and chaos that the Internet represents.

- Robert Lacey, author of "The Kingdom," about the Saudi royal family

"It's a good question," says Hatoon Al Fassi, a political activist and a history professor at King Saud University. "Everybody, politically speaking, is on their nerves," she says, "and they are not happy with anything that goes on in the media."

Fassi says she felt the chill firsthand when she delivered her weekly column to *Al-Riyadh* newspaper. Fassi's comments on the Arab government response to events in Tunisia were rejected at first.

She says she told her editor, "Everything I've written was actually from the news; I haven't put anything new." But, she says, her editor pointed out that she had put all the information together and cited reforms in neighboring Gulf states.

New Rules In Effect

While Saudi Arabia still can control the domestic media, it's harder to block out international news, with Arab satellite channels and constant updates on blogs and Twitter feeds.

But for the first time, the Saudi government has published new regulations for the electronic media, which includes bloggers. All users are encouraged to register with the government and the new rules, in effect since Jan. 1, prohibit criticism of Islam or anything that compromises public order.

The new rules have spurred an outburst of criticism online.

Social Media Revolution Hits Saudi Arabia



saudialchemist.org

A screenshot of saudialchemist.org, taken on Jan. 26, 2011.

"I believe this is an ugly tactic of censoring freedom of expression," says Mohammed Qatani, the head of the Saudi Civil and Political Rights Association, an unofficial human-rights group. SCPA published provocative challenges to the government, including calling for the resignation of the interior minister. The association has registered the site outside the kingdom.

"They do censor our website," says Qatani. "Over the past year it has been blocked more than 15 times. ... Every two weeks, they shut it down. But we figure out how to [get around it]."

But the Saudi government has harassed and jailed critics, according to Human Rights Watch. In a new report issued this week, Human Rights Watch warns that the new regulations are likely to suppress electronic communication after Saudi Arabia's Web users have opened a space for a lively exchange of views on the Web.

However, Prince Turki al Faisal, a former head of intelligence and diplomat, insists that this is no clampdown.

"If you want to get to a certain website, who can prevent you? You can hook your phone to a provider in Ukraine or Timbuktu," he says. "It is not a means to clamp down, but simply to regulate them."

Social Media Revolution Hits Saudi Arabia

An Alternative News Source

The Saudi blogosphere has become an alternative source of news and opinions in the kingdom. Even government officials check on blog sites as a source of information.



nofah.com/wordpress

A screenshot of nofah.com/wordpress taken on Jan. 26, 2011.

In 2009, postings on YouTube about a devastating flood that killed 70 people alerted government officials to the extent of the crisis.

Robert Lacey has lived in Saudi Arabia for decades and wrote a best-selling book about the royal family.

"The young Saudis I've spoken to about this plan to get bloggers registered just laugh," he says. "There are all sorts of technical ways that I don't quite understand — blogging under an assumed name."

Lacey says the Internet poses a challenge for this conservative, mostly religious society.

"It's one of the big questions ahead for Saudi Arabia," he says. "How this authoritarian regime will live with the freedom and chaos that the Internet represents."

Can Governments Really 'Block' Twitter?

Can Governments Really 'Block' Twitter?

Not really. The domain name is inaccessible, but it's not that hard to get around.

BY JOSHUA E. KEATING | JANUARY 26, 2011

This week, Egypt became the latest Middle Eastern country to see massive anti-government street demonstrations. As in Tunisia earlier this month and Iran last year, activists have made heavy use of social networking sites like **Twitter** and **Facebook** -- and the Egyptian regime has responded harshly. On Jan. 25, Twitter **officially confirmed** reports that access to its site had been blocked. Is it really possible to do that?

Yes, but not very effectively. The Egyptian government appears to have been blocking access to the Twitter.com domain name, most likely with the assistance of the country's Internet-service **monopoly TE Data**. Later in the day on Tuesday, Egyptian authorities began shutting down wireless data services entirely in the areas where the protests were taking place in order to prevent demonstrators from logging on. (Facebook has also reportedly been **suffering outages** on Jan. 26, though the company denies that it **has been blocked**.) As is **its habit**, the Egyptian government hasn't created a redirect page for the site, but merely slowed traffic down to a crawl to give itself plausible deniability. Late in the day on Jan. 26, the site was reportedly accessible again.

Unfortunately for the censors, Twitter allows other companies to develop their own applications using its **programming interface**. This has led to the development of a plethora of tools that allow users to post to Twitter without ever pointing their browsers to Twitter.com. These third-party clients still appear to be functioning in Egypt. There have even been reports of activists updating Twitter through the professional résumé-sharing site LinkedIn.

It's also still not prohibitively difficult to access Twitter.com. The site has multiple IP addresses, not all of which are blocked by government censors. Savvier Egyptian web

Can Governments Really 'Block' Twitter?

users can access one of these addresses without using the site's domain name at all. Another easy workaround is to use a virtual private network, or VPN, which fools the system into thinking you're outside Egypt.

Unlike other authoritarian states such as China or Iran, Egypt does not have a particularly extensive web-filtering operation in place. The decision to block Twitter may be a sign of how serious the regime is taking the protests, though even now the restrictions seem somewhat haphazard and arbitrary. For instance, while Bambuser, a site used to stream video to one's Facebook account from a mobile phone, **has been blocked**, YouTube, which has been used extensively by the protesters, is **still accessible**.

Some regimes have been more aggressive in counteracting the effects of social networking. During the Tunisian protests, a malicious program hosted by the country's Internet service providers was **found to be stealing** users' login information and passwords. In 2009, a group calling itself the Iranian Cyber Army, thought to have links to the Iranian government, hacked Twitter so that it instead displayed anti-American propaganda.

Generally, the Egyptian authorities **prefer** to allow opposition members to share information online so that they can closely monitor them. In some cases, they've gone as far as to ask online activists for their email and website passwords rather than shutting them down. But with riots spreading throughout the Arab world in the wake of Tunisia, the powers-that-be may have decided that blunter methods were called for.

*Thanks to Mark Belinsky, co-director of **Digital Democracy**, and Ethan Zuckerman, senior researcher at the **Berkman Center for Internet and Society at Harvard***

Can Governments Really 'Block' Twitter?

University.

The Internet Dies in Egypt

The Internet Dies in Egypt, in Pictures

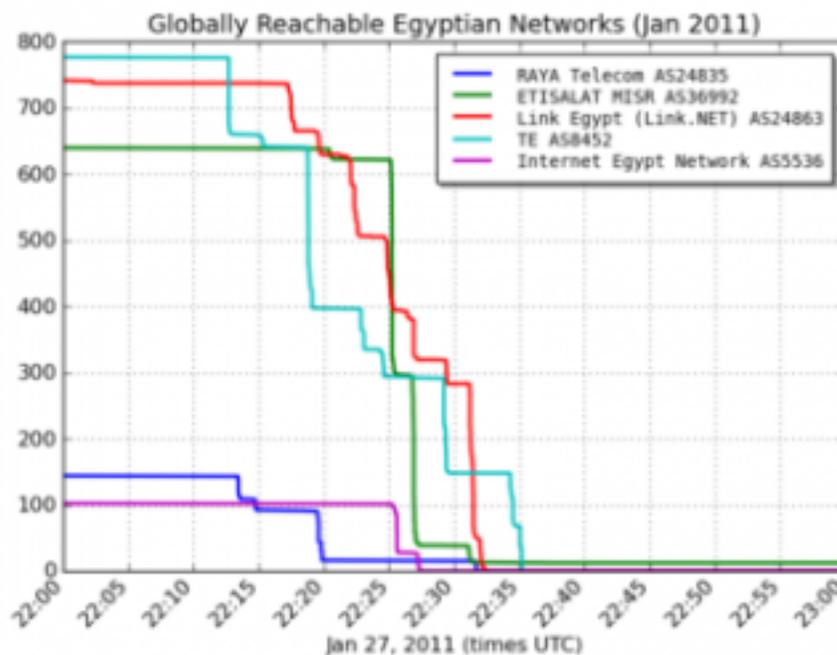
by Liz Gannes

Posted on January 28, 2011 at 10:29 AM PT

Graphic images and videos of violence and swarms of protesters in Egypt have helped communicate the impact of anti-government demonstrations to the world. The near-total shutdown of Egyptian Internet access is also something that benefits from illustration.

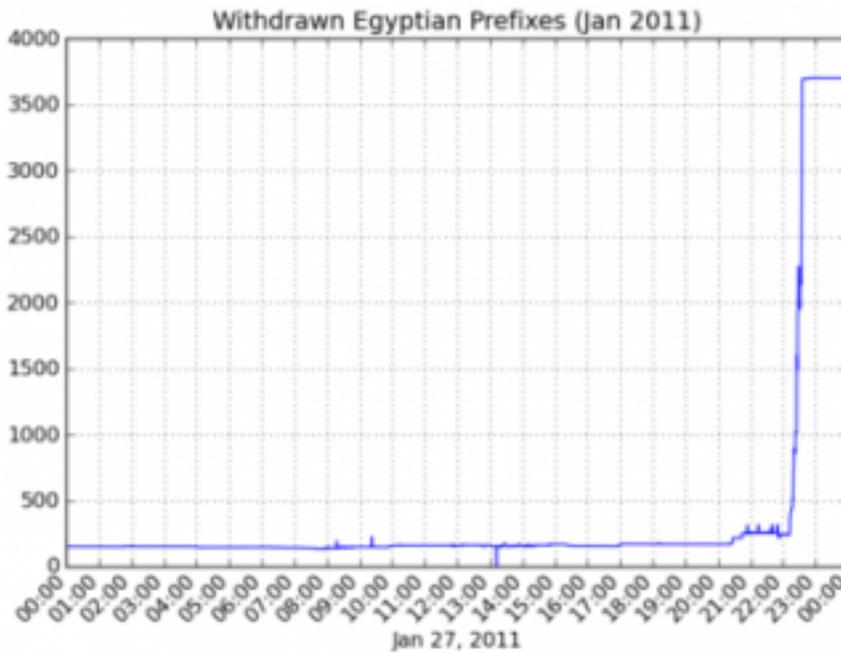
What exactly Egypt did to cut online access isn't that well-understood—the [informed hypothesis](#) we've seen indicates that the government made phone calls to the nation's major providers, shutting down all of them but one and making 93 percent of Egyptian networks unavailable.

Here's a chart that shows that process, via Internet routing analytics firm Renesys:



And here's Renesys' illustration of withdrawn Internet prefixes:

The Internet Dies in Egypt

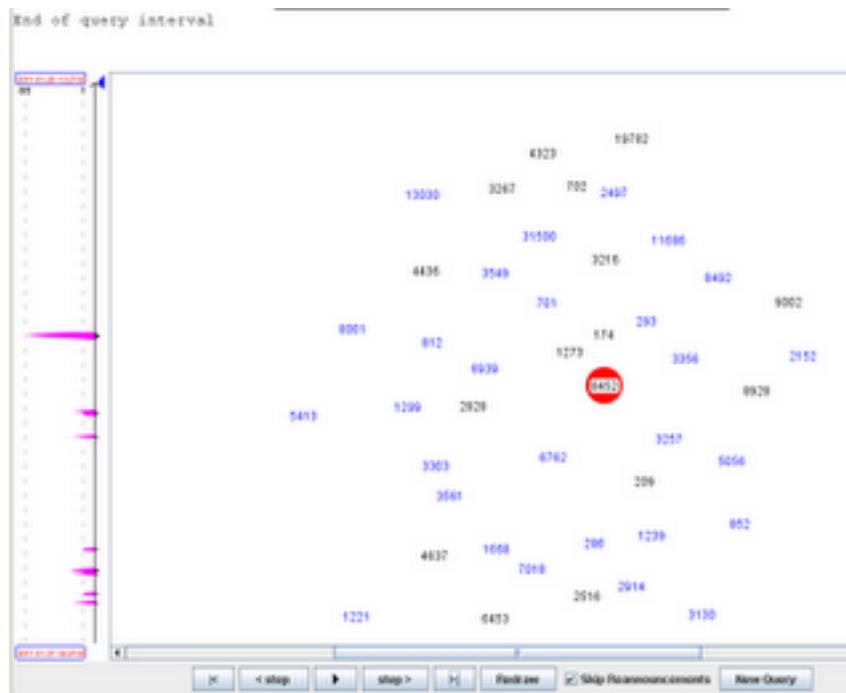
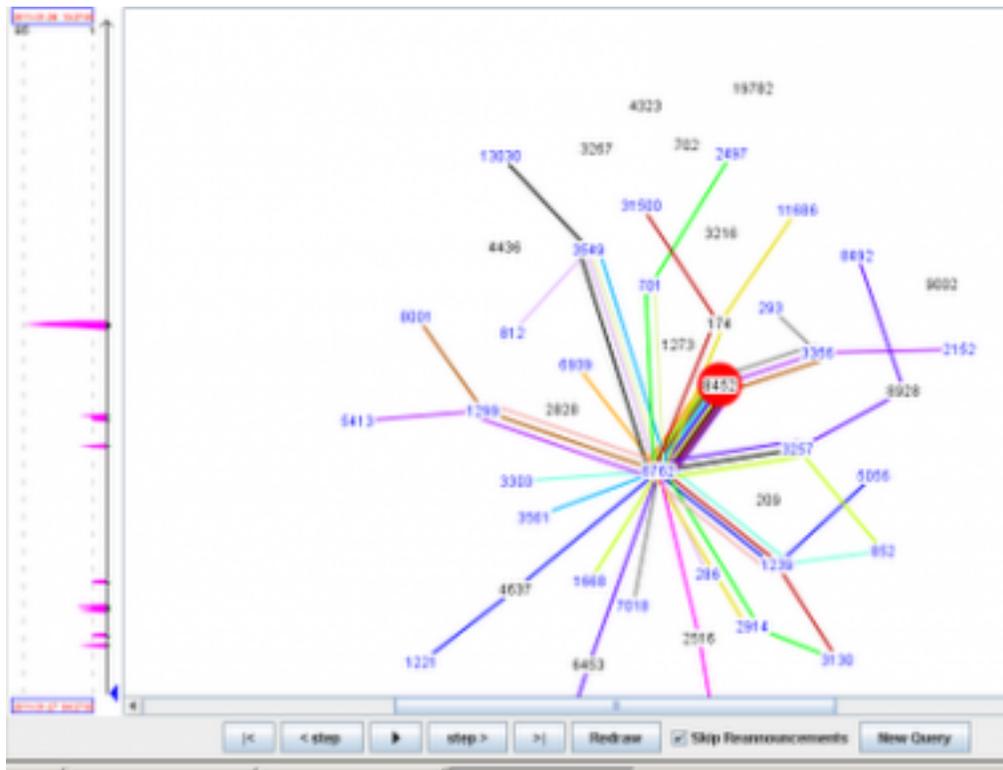


Here's network security provider Arbor Networks' [illustration](#) of the dramatic drop of traffic to Egypt:



And here's a before-and-after visualization of Internet routing in Egypt published on the blog [Extra Exploit](#).

The Internet Dies in Egypt



The Internet Dies in Egypt

Egypt's Web, Mobile Communications Severed

Egypt's Web, Mobile Communications Severed

By [SHEREEN EL GAZZAR](#), [LILLY VITOROVICH](#) And [RUTH BENDER](#)

The Egyptian government's crackdown on protestors intensified Friday with access to most forms of mass communication, including the Internet, mobile and SMS down, even as United Nations Secretary General Ban Ki-moon warned that "freedom of expression should be fully respected."

As the country braced for huge antigovernment protests on the traditional day of prayer, the government appeared to have unplugged most means of communication—including social network Facebook and Twitter—that activists had been using to coordinate action across the country. Landline calls placed from outside the country, however, were connecting.

Government-owned Telecom Egypt runs the country's fixed-line network. Attempts to connect to the websites of several Egyptian ISPs, including EgyptWeb, TeData and Purenet all failed.

U.K.-headquartered Vodafone Group PLC said in a statement that all mobile operators in Egypt had been "instructed to suspend services in parts of Egypt. Under Egyptian legislation, the authorities have the right to issue such an order and we are obliged to comply with it." It said the Egyptian authorities will be clarifying the situation in due course.

Vodafone CEO Vittorio Colao said in comments to a Davos session on mobile devices that "Egyptian authorities" had asked the company to "turn down the network totally."

Mr. Colao said Vodafone determined that the request was legitimate under Egyptian law, and therefore complied with the request. "I hope" the decision will be reversed by Egypt "very soon," Mr. Colao said.

In a blog, U.S.-based Internet intelligence firm Renesys recorded how late Thursday it saw "the virtually simultaneous withdrawal of all routes to

Egypt's Web, Mobile Communications Severed

Egyptian networks in the Internet's global routing table," in what it called "an action unprecedented in Internet history."

It contrasted the scale of the crackdown with the "modest Internet manipulation that took place in Tunisia, where specific routes were blocked, or Iran, where the Internet stayed up," but download times were slowed.

During the rallies in Iran in 2009, one account from a person in the capital, Tehran, said it took 20 minutes to download Yahoo's website and that landlines, satellite phones and SMS were all disrupted.

And in 2007, security forces in Myanmar cracked down on communications following monk-led protests against the regime there, disabling some mobile phones and closing some service providers, but images of the clampdown continued to be relayed out of the country via cellphones. More than 110,000 people joined the Support the Monk's Protest in Burma group on Facebook. Facebook and Twitter weren't immediately available to comment on what is happening in Egypt.

France Telecom also confirmed that the Egyptian authorities had taken "measures to block mobile phone services," and apologized to Mobinil customers, adding it had no information about when service would be restored.

All attempts to reach other mobile and Internet operators in the country were unsuccessful either because offices were closed due to the weekend or because mobile numbers weren't working.

"From my knowledge of the region, I suspect the Egyptian government controls the main ISP in the country and would thus be able to decouple the main backbone in Egypt from the rest of the Internet," said Sean Sullivan, security adviser at Finnish IT security firm F-Secure. Mr. Sullivan drew parallels with Syria, where the government also has full control of the Internet

Egypt's Web, Mobile Communications Severed

backbone and can therefore shut down the network if it wishes.

Egyptians Protest Again

"It's a blunt instrument to fight what is happening" in Egypt, Mr. Sullivan said, referring to the communications clampdown, but people in the country seemed to be finding alternatives to get news out to the world, for example via satellite connections or by placing calls to friends who then tweet for them.

According to Egypt's National Telecom Regulatory Authority, or NTRA, mobile subscribers in the country reached 53.43 million by the end of the third quarter of 2010, the latest figures available.

Earlier this week, blogs and social networks were full of calls to take to the streets to bring down the regime of Egyptian President Hosni Mubarak. Egypt's Interior Ministry had warned it would take decisive measures against the protestors in the Arab world's most populous nation, after organizers said demonstrations set to take place after noon prayers Friday would be the biggest in decades.

The protests in Egypt come after the 25-year regime of Zine El Abidine Ben Ali was toppled in Tunisia, sparking shockwaves across the Arab world.

Egypt's Leaders Found 'Off' Switch for the Internet

Egypt Leaders Found 'Off' Switch for Internet

By **JAMES GLANZ** and **JOHN MARKOFF**

Epitaphs for the Mubarak government all note that the mobilizing power of the Internet was one of the Egyptian opposition's most potent weapons. But quickly lost in the swirl of revolution was the government's ferocious counterattack, a dark achievement that many had thought impossible in the age of global connectedness. In a span of minutes just after midnight on Jan. 28, a technologically advanced, densely wired country with more than 20 million people online was essentially severed from the global Internet.

The blackout was lifted after just five days, and it did not save President Hosni Mubarak. But it has mesmerized the worldwide technical community and raised concerns that with unrest coursing through the Middle East, other autocratic governments — many of them already known to interfere with and filter specific Web sites and e-mails — may also possess what is essentially a kill switch for the Internet.

Because the Internet's legendary robustness and ability to route around blockages are part of its basic design, even the world's most renowned network and telecommunications engineers have been perplexed that the Mubarak government succeeded in pulling the maneuver off.

But now, as Egyptian engineers begin to assess fragmentary evidence and their own knowledge of the Egyptian Internet's construction, they are beginning to understand what, in effect, hit them. Interviews with many of those engineers, as well as an examination of data collected around the world during the blackout, indicate that the government exploited a devastating combination of vulnerabilities in the national

Egypt's Leaders Found 'Off' Switch for the Internet

infrastructure.

For all the Internet's vaunted connectivity, the Egyptian government commanded powerful instruments of control: it owns the pipelines that carry information across the country and out into the world.

Internet experts say similar arrangements are more common in authoritarian countries than is generally recognized. In Syria, for example, the Syrian Telecommunications Establishment dominates the infrastructure, and the bulk of the international traffic flows through a single pipeline to Cyprus. Jordan, Qatar, Oman, Saudi Arabia and other Middle Eastern countries have the same sort of dominant, state-controlled carrier.

Over the past several days, activists in Bahrain and Iran say they have seen strong evidence of severe Internet slowdowns amid protests there. Concerns over the potential for a government shutdown are particularly high in North African countries, most of which rely on a just a small number of fiber-optic lines for most of their international Internet traffic.

A Double Knockout

The attack in [Egypt](#) relied on a double knockout, the engineers say. As in many authoritarian countries, Egypt's Internet must connect to the outside world through a tiny number of international portals that are tightly in the grip of the government. In a lightning strike, technicians first cut off nearly all international traffic through those portals.

In theory, the domestic Internet should have survived that strike. But the cutoff also

Egypt's Leaders Found 'Off' Switch for the Internet

revealed how dependent Egypt's internal networks are on moment-to-moment information from systems that exist only outside the country — including e-mail servers at companies like [Google](#), [Microsoft](#) and [Yahoo](#); data centers in the United States; and the Internet directories called domain name servers, which can be physically located anywhere from Australia to Germany.

The government's attack left Egypt not only cut off from the outside world, but also with its internal systems in a sort of comatose state: servers, cables and fiber-optic lines were largely up and running, but too confused or crippled to carry information save a dribble of local e-mail traffic and domestic Web sites whose Internet circuitry somehow remained accessible.

“They drilled unexpectedly all the way down to the bottom layer of the Internet and stopped all traffic flowing,” said Jim Cowie, chief technology officer of [Renesys](#), a network management company based in New Hampshire that has [closely monitored Internet traffic from Egypt](#). “With the scope of their shutdown and the size of their online population, it is an unprecedented event.”

The engineers say that a focal point of the attack was an imposing building at 26 Ramses Street in Cairo, just two and a half miles from the epicenter of the protests, Tahrir Square. At one time purely a telephone network switching center, the building now houses the crucial Internet exchange that serves as the connection point for fiber-optic links provided by five major network companies that provide the bulk of the Internet connectivity going into and out of the country.

“In Egypt the actual physical and logical connections to the rest of the world are few, and

Egypt's Leaders Found 'Off' Switch for the Internet

they are licensed by the government and they are tightly controlled,” said Wael Amin, president of ITWorx, a large software development company based in Cairo.

One of the government’s strongest levers is [Telecom Egypt](#), a state-owned company that engineers say owns virtually all the country’s fiber-optic cables; other Internet service providers are forced to lease bandwidth on those cables in order to do business.

Mr. Cowie noted that the shutdown in Egypt did not appear to have diminished the protests — if anything, it inflamed them — and that it would cost untold millions of dollars in lost business and investor confidence in the country. But he added that, inevitably, some autocrats would conclude that Mr. Mubarak had simply waited too long to bring down the curtain.

“Probably there are people who will look at this and say, it really worked pretty well, he just blew the timing,” Mr. Cowie said.

Speaking of the Egyptian shutdown and the earlier experience in Tunisia, whose censorship methods were less comprehensive, a senior State Department official said that “governments will draw different conclusions.”

“Some may take measures to tighten communications networks,” said the official, speaking on the condition of anonymity. “Others may conclude that these things are woven so deeply into the culture and commerce of their country that they interfere at their peril. Regardless, it is certainly being widely discussed in the Middle East and North Africa.”

Egypt's Leaders Found 'Off' Switch for the Internet

Vulnerable Choke Points

In Egypt, where the government still has not explained how the Internet was taken down, engineers across the country are putting together clues from their own observations to understand what happened this time, and to find out whether a future cutoff could be circumvented on a much wider scale than it was when Mr. Mubarak set his attack in motion.

The strength of the Internet is that it has no single point of failure, in contrast to more centralized networks like the traditional telephone network. The routing of each data packet is handled by a web of computers known as routers, so that in principle each packet might take a different route. The complete message or document is then reassembled at the receiving end.

Yet despite this decentralized design, the reality is that most traffic passes through vast centralized exchanges — potential choke points that allow many nations to monitor, filter or in dire cases completely stop the flow of Internet data.

China, for example, has built an elaborate national filtering system known as the Golden Shield Project, and in 2009 it shut down cellphone and Internet service amid unrest in the Muslim region of Xinjiang. Nepal's government briefly disconnected from the Internet in the face of civil unrest in 2005, and so did Myanmar's government in 2007.

But until Jan. 28 in Egypt, no country had revealed that control of those choke points could allow the government to shut down the Internet almost entirely.

There has been intense debate both inside and outside Egypt on whether the cutoff at

Egypt's Leaders Found 'Off' Switch for the Internet

26 Ramses Street was accomplished by surgically tampering with the software mechanism that defines how networks at the core of the Internet communicate with one another, or by a blunt approach: simply cutting off the power to the router computers that connect Egypt to the outside world.

But either way, the international portals were shut, and the domestic system reeled from the blow.

The Lines Go Dead

The first hints of the blackout had actually emerged the day before, Jan. 27, as opposition leaders prepared for a “Friday of anger,” with huge demonstrations expected. Ahmed ElShabrawy, who runs a company called EgyptNetwork, noticed that the government had begun blocking individual sites like [Facebook](#) and [Twitter](#).

Just after midnight on Jan. 28, Mahmoud Amin’s [iPhone](#) beeped with an alert that international connections to his consulting company’s Internet system had vanished — and then the iPhone itself stopped receiving e-mail. A few minutes later, Mr. ElShabrawy received an urgent call telling him that all Internet lines running to his company were dead.

It was not long before Ayman Bahaa, director of Egyptian Universities Network, which developed the country’s Internet nearly two decades ago, was scrambling to figure out how the system had all but collapsed between the strokes of 12 and 1.

The system had been crushed so completely that when a network engineer who does

Egypt's Leaders Found 'Off' Switch for the Internet

repairs in Cairo woke in the morning, he said to his family, “I feel we are in the 1800s.”

Over the next five days, the government furiously went about extinguishing nearly all of the Internet links to the outside world that had survived the first assault, data collected by Western network monitors show. Although a few Egyptians managed to post to Facebook or send sporadic e-mails, the vast majority of the country’s Internet subscribers were cut off.

The most telling bit of evidence was that some Internet services inside the country were still working, at least sporadically. [American University in Cairo](#), frantically trying to relocate students and faculty members away from troubled areas, was unable to use e-mail, cellphones — which were also shut down — or even a radio frequency reserved for security teams. But the university was able to update its Web site, hosted on a server inside Egypt, and at least some people were able to pull up the site and follow the emergency instructions.

“The servers were up,” said Nagwa Nicola, the chief technology officer at American University in Cairo. “You could reach up to the Internet provider itself, but you wouldn’t get out of the country.” Ms. Nicola said that no notice had been given, and she depicted an operation that appeared to have been carried out with great secrecy.

“When we called the providers, they said, ‘Um, hang on, we just have a few problems and we’ll be on again,’ ” she said. “They wouldn’t tell us it was out.”

She added, “It wasn’t expected at all that something like that would happen.”

Egypt's Leaders Found 'Off' Switch for the Internet

Told to Shut Down or Else

Individual Internet service providers were also called on the carpet and ordered to shut down, as they are required to do by their licensing agreements if the government so decrees.

According to an Egyptian engineer and an international telecom expert who both spoke on the condition of anonymity, at least one provider, [Vodafone](#), expressed extreme reluctance to shut down but was told that if it did not comply, the government would use its own “off” switch via the Telecom Egypt infrastructure — a method that would be much more time-consuming to reverse. Other exchanges, like an important one in Alexandria, may also have been involved.

Still, even major providers received little notice that the moves were afoot, said an Egyptian with close knowledge of the telecom industry who would speak only anonymously.

“You don’t get a couple of days with something like this,” he said. “It was less than an hour.”

After the Internet collapsed, Mr. ElShabrawy, 35, whose company provides Internet service to 2,000 subscribers and develops software for foreign and domestic customers, made urgent inquiries with the Ministry of Communications, to no avail. So he scrambled to re-establish his own communications.

When he, too, noticed that domestic fiber-optic cables were open, he had a moment of exhilaration, remembering that he could link up servers directly and establish

Egypt's Leaders Found 'Off' Switch for the Internet

messaging using an older system called Internet Relay Chat. But then it dawned on him that he had always assumed he could download the necessary software via the Internet and had saved no copy.

“You don’t have your tools — you don’t have anything,” Mr. ElShabrawy said he realized as he stared at the dead lines at his main office in Mansoura, about 60 miles outside Cairo.

With the streets unsafe because of marauding bands of looters, he decided to risk having a driver bring \$7,000 in satellite equipment, including a four-foot dish, from Cairo, and somehow he was connected internationally again by Monday evening.

Steeling himself for the blast of complaints from angry customers — his company also provides texting services in Europe and the Middle East — Mr. ElShabrawy found time to post videos of the protests in Mansoura on his Facebook page. But with security officials asking questions about what he was up to, he did not dare hook up his domestic subscribers.

Then, gingerly, he reached out to his international customers, his profuse apologies already framed in his mind.

The response that poured in astonished Mr. ElShabrawy, who is nothing if not a conscientious businessman, even in turbulent times. “People said: ‘Don’t worry about that. We are fine and we need to know that you are fine. We are all supporting you.’ ”

Wary of Egypt Unrest, China Sensors Web

Wary of Egypt Unrest, China Censors Web

By [EDWARD WONG](#) and [DAVID BARBOZA](#)

Published: January 31, 2011

BEIJING — In another era, China’s leaders might have been content to let discussion of [the protests in Egypt](#) float around among private citizens, then fizzle out.

But challenges in recent years to authoritarian governments around the globe and violent uprisings in parts of China itself have made [Chinese officials increasingly wary](#) of leaving such talk unchecked, especially on the Internet, the medium some officials see as central to fanning the flames of unrest.

So the arbiters of speech sprang into action over the weekend. Sina.com and Netease.com — two of the nation’s biggest online portals — blocked keyword searches of the word “Egypt,” though the mass protests were being discussed on some Internet chat rooms on Monday. Searching for “Egypt” has also been blocked on Weibo, the Chinese equivalent of [Twitter](#).

Censoring the Internet is not the only approach. The Chinese government has also tried to get out ahead of the discussion, framing the Egyptian protests in a few editorials and articles in state-controlled news publications as a [chaotic affair](#) that embodies the pitfalls of trying to plant democracy in countries that are not quite ready for it — a line China’s leaders have long held.

The English-language edition of Global Times, a populist newspaper, ran an editorial on Sunday about the Tunisian and Egyptian protests with the headline “[Color revolutions will not bring about real democracy](#).” Though Global Times is not the official mouthpiece of the Communist Party, the message of the editorial was consistent with official thinking, saying bluntly that whether democracy “is applicable in other countries is in

Wary of Egypt Unrest, China Sensors Web

question, as more and more unsuccessful examples arise.”

“The official Chinese media is reporting the Egypt events — it’s no longer possible for Xinhua and other official media to remain credible if they hide international news that people can learn from the Internet,” said Susan L. Shirk, a professor at the University of California, San Diego, who served as assistant deputy secretary of state during the Clinton administration. “But they reduce the risk that some Chinese might want to emulate them by describing them as 'anti-government riots.'”

Some Chinese news organizations have also seized on the ambivalent American reaction to the Egyptian unrest to underscore the hypocrisy of the United States in sometimes backing dictators over democracy. They argued that those who appear to be the greatest advocates of democracy sometimes have conflicted feelings about its spread, especially in the Middle East, where the United States fears the proliferation of populist radical Islam. China Youth Daily noted in an editorial on Sunday that “the increasing turmoil in Egypt is causing a ‘headache’ for the decision makers in Washington.”

Some of the news coverage of Egypt that has appeared in People’s Daily, the Communist Party’s main newspaper, and Xinhua, the official news agency, has focused on attempts by China to evacuate its citizens, simply leaving out the political discontent at the root of the unrest. Xiao Qiang, an adjunct professor at the [University of California, Berkeley](#), and an expert on Internet censorship in China, said propaganda officials had recently ordered Chinese news organizations and Web sites to strictly follow Xinhua reports on Egypt.

But Mr. Xiao said some Internet forums were closely tracking the events in Egypt. “I can see the Egypt story being followed and discussed by active netizens everywhere — blogs, forums, social networking services like Kaixin and Renren,” he said. “It’s just not on the

Wary of Egypt Unrest, China Sensors Web

front page of major Web sites.”

The Chinese authorities’ efforts to censor and shape news on the Internet have evolved over the past few years, as they grappled with unrest during the Tibet riots in 2008 and protests against the [Olympic torch](#) relay. The authorities initiated a crackdown on pornography and other “harmful information,” including shuttering a popular liberal forum, soon after the release of Charter 08, an online manifesto calling for gradual democratic reforms that gathered thousands of signatures through e-mail.

Internet controls ramped up in late 2009, when officials observed how social networking sites and other forums helped inflame unrelated outbursts of protests and rioting in Iran and Xinjiang, the restive region in China’s west.

In an August 2009 article on the Iran protests, a monthly journal published by the central propaganda department warned of the challenge posed by sites like Twitter and [Facebook](#), which the authorities had blocked days after riots in Xinjiang. In January 2010, after Secretary of State [Hillary Rodham Clinton](#) announced a new United States policy to counter online censorship abroad, an editorial published by People’s Daily charged that the United States had used the Internet — YouTube and Twitter in particular — to stir up “online warfare” against [Mahmoud Ahmadinejad](#), the Iranian president.

The Internet’s influence on the volatile events in Iran and Xinjiang “impacted the leadership like an earthquake,” said one media investor with high-level ties to China’s regulators who spoke on the condition of anonymity for fear of damaging that relationship.

The fact that social networking sites have fueled the protests in Egypt will no doubt spur Chinese officials to further scrutinize such sites. And they may be right to pay attention:

Wary of Egypt Unrest, China Sensors Web

Zhao Jing, a liberal Chinese blogger who goes by the name of Michael Anti, said that “it was amazing netizens on Twitter cared about Egypt so much” that they had begun drawing parallels between China and Egypt. President [Hosni Mubarak](#) of Egypt was being called Mu Xiaoping, a reference to [Deng Xiaoping](#), who quashed the 1989 popular protests in Beijing, while Tahrir Square in Cairo was being compared to Tiananmen Square.

Yet, there are intellectuals in Beijing skeptical of any similar protests arising in China, mainly because this nation’s dynamic economy has given many Chinese hope for a better life.

“I don’t think dissemination of such news would cause unrest in China,” said Jia Qingguo, associate dean of international relations at Peking University. “Egypt is a different type of political regime from China. They are also not a socialist country. They have their own particular problems.”

Edward Wong reported from Beijing, and David Barboza from Shanghai. Jonathan Ansfield contributed reporting from Beijing. Chen Xiaoduan contributed research in Shanghai.

Where Innovation Is Sorely Needed

Where Innovation Is Sorely Needed

The pervasiveness of data threatens to upend some business models and enhance others.

By Paul B. Carroll and Chunka Mui

Everyone recognizes that technology is destroying long-standing business models in news, music, and other media industries, but the next few years could also bring wracking changes in numerous other businesses, such as insurance, retail, cars, medicine, toys, and utilities.

The reason lies in the third wave of personal computing. The first, beginning in the late 1970s, gave us PCs. The second, the Internet revolution of the 1990s, hooked all those computers together. The third is letting us essentially carry the Internet with us, on smart phones, tablets, and other devices. Cameras and sensors are becoming cheap and ubiquitous. Every person and device will be able to talk to any other person or device, anytime and anywhere. And operating in this world of infinite connections will change almost everything for businesses.

Those accustomed to broadcasting their messages will have to get comfortable in the middle of a conversation where everyone is talking to everyone else, all at the same time. Businesses that act as middlemen will have to justify their value or get pushed aside. Businesses that depend on market ignorance will have to adjust to total transparency on price and quality. And that's just for starters.

For example, because sensors, cameras, and wireless connections will be active in cars or in the smart phones that drivers and passengers carry, auto insurance will increasingly be based on detailed real-time information, such as how many miles are actually driven, how fast the car is going, and whether the driver stops at stop signs and uses turn signals.

Insurers will need to respond with far more flexible and customized pricing than they offer now. Allstate, Progressive, and others are already offering "Pay-As-You-Drive" programs that offer lower rates to (presumably safer) drivers who allow them to monitor such information. Insurers may also communicate more with customers in an effort to reduce claims. For instance, they might warn that a customer's teenage son has deviated from the approved route from school and has seven friends in the car. Teens have accidents at about twice the rate of other drivers; any company that can prevent some of those accidents has the opportunity to lower individual premiums and capture much of the \$20 billion in overall premiums that teens represent in the United States

Where Innovation Is Sorely Needed

each year.

The story will be similar in other industries. For example:

- Retail stores. Physical stores will face increased price and quality pressure because of apps like Red Laser, which displays reviews for a product, and the prices it's selling for at neighboring stores and online, when the customer uses a smart phone to scan the bar code. Malls and physical retailers have long clung to the notion that once customers are in the store, they will want the immediate gratification of buying a product and taking it home. Yet with unlimited information about alternatives at their fingertips, more in-store shoppers might choose savings and free shipping from a cheaper supplier. It might not be long before location-based capabilities yield another level of price competition. For instance, Amazon could offer an additional 5 percent off to shoppers browsing its site from inside a Walmart store.
- Cars. There's a saying that car companies make cars while everyone else makes money (on financing, warranties, repairs, insurance, and so on). But car companies could move in on these money-making opportunities by capturing usage and diagnostic data in real time. GM, for example, is already offering discounted insurance to customers of its OnStar remote security system.
- Medicine. Health-care providers will have to switch from seeing patients episodically to seeing them, in essence, every moment of the day. Even now, implantable sensors for people with heart problems can send a steady stream of data through a wireless device to a doctor's office for evaluation. Over time, as sensors and wireless devices spread, doctors (or, more accurately, their computers) will start monitoring many patients for a whole array of health issues. The data will find its way into the public domain in some form, making it possible for patients to know which doctors are especially effective and creating new types of competition.
- Utilities. Utilities, which have barely innovated for decades, are now adding sensors throughout the electric grid and putting "smart" meters in homes and businesses to manage the grid more efficiently and get a better sense of demand. They will have to be able to vary the retail price of electricity in real time and relay that information to consumers and businesses instantly, so they can adjust their usage to limit demand when prices are high. Some utilities will handle the transition well, but many will not.
- Toys. Kids are migrating to higher-technology content earlier. That may be bad news for companies that sell dolls and blocks, but it's good for those that provide entertainment on smart phones and tablets. Already, the social aspects of such

Where Innovation Is Sorely Needed

devices are creating opportunities for innovators to reinvent toys and games. For example, many people now use phones to play a game of Scrabble over the course of several days, making a move whenever they have time.

The companies that operate in this new world had better be smart. Tomorrow, we'll lay out key principles on what it takes.

*Paul B. Carroll and Chunka Mui are cofounders and managing directors of **Devil's Advocate Group**, a consultancy that helps businesses test their innovation strategies. They are also coauthors of Billion-Dollar Lessons: What You Can Learn From the Most Inexcusable Business Failures of the Last 25 Years.*

Four Principles for Crafting Your Innovation Strategy

Four Principles for Crafting Your Innovation Strategy

Two management consultants explain what successful companies have done to prepare for a world of constant Internet connectivity.

By Paul B. Carroll and Chunka Mui

The economist Joseph Schumpeter coined the term "creative destruction" in the late 1930s—long before Moore's law and the creative destruction that was unleashed by a doubling of computing power every 18 months. Compared with the events of recent decades, what Schumpeter saw was creative destruction in slow motion. And the pace of innovation has picked up markedly in the last five years, because the spread of smart phones, tablets, and other mobile devices is letting us all take the incredible power of the Internet with us wherever we go.

To come out ahead, companies should follow four principles:

Think big, start small, fail quickly, scale fast.

Even as he built the DVD business that toppled Blockbuster, Netflix CEO Reed Hastings was guided by the big idea that mailing people DVDs was a mere way station on the road to streaming movies directly into people's homes. The market is now richly rewarding Netflix for being on the cusp of achieving this vision, but what Hastings should get credit for is how diligently he prepared for this day.

As far back as 2001, Hastings spent \$10 million on research into streaming; he was willing to forgo most of his small company's profits to get started on his preparation. In the years since, Hastings has frequently prepared to offer streaming video—only to junk the projects when he realized they weren't feasible. As streaming started to become real, Hastings did a host of deals with content providers to see which would work and to make sure he wasn't left out, even though it was clear that most of the deals wouldn't amount to much. Hastings also considered numerous pricing models for streaming and ultimately decided to start by giving it away as part of DVD subscriptions. That way, people could get used to streaming while he built his library of offerings, and he wouldn't create an opening for a competitor.

In late 2010, after almost 10 years of experimentation, he offered a streaming-only option for about half the price of a subscription for DVDs by mail. That, combined with the increasing size of the library, should accelerate the move to streaming.

Hastings had a grand vision from the outset, but he started with lots of small projects

Four Principles for Crafting Your Innovation Strategy

that often failed and that he killed quickly. Now he's scaling fast and reaping the benefits of his diligent approach to innovation in confusing times.

Many companies are not very good at this process. In particular, they can't seem to start small because senior management won't pay attention to small projects. Companies also aren't very good at failing quickly. Instead, they tend to swing between complacency and panic. They wait until they're way behind and then bet everything on one big idea. And, as one senior executive has told us, "the only thing harder than starting a strategic initiative is killing one." Once something gets under way, too many people are invested in it for it to go away easily.

Start with a clean sheet of paper.

At the moment, malls have a huge disadvantage relative to online stores. Electronic retailers have detailed knowledge of a prospective customer's preferences and purchase history, while those in malls generally can know nothing about their customers until they present a credit card at the register. At that point, it's too late to personalize promotions or shape the shopping experience.

New connected technology is giving heretofore "offline" malls and stores a chance to reimagine how they interact with customers. The first step is getting customers to identify themselves using their smart phones. Some customers already do so through social apps such as Foursquare and Facebook Places. Others do so when offered small incentives through loyalty programs such as Shopkick, which gives shoppers points when they check in at participating malls, like many of those operated by Simon Property Group, and at retailers, like Best Buy and Crate & Barrel.

Building on this newfound identity and location information, and leveraging social media, malls and stores are starting to create social experiences that are not possible online. Eventually, a group of teenage girls might go to a store and disperse but keep track of each other through the GPS on their phones. They'd identify themselves through the mall loyalty program and be treated to a slew of customized promotions based on their preferences and buying histories. The girls would keep up with each other via Facebook, tweets, or texts and gather periodically as someone finds an interesting item or person. They could attract other friends to the mall. A movie theater, practicing yield management the way airlines do, might entice some of the girls with cheap tickets rather than have seats go vacant. The whole mall experience could become an adventure.

By contrast, the descent of Blockbuster during the last decade shows what can happen

Four Principles for Crafting Your Innovation Strategy

when a company isn't imaginative enough about the new possibilities of a technology. To be fair, Blockbuster didn't have an easy task in front of it. It had thousands of stores, many owned by franchisees who had rights that restricted how quickly Blockbuster could change. Still, Blockbuster apparently never even imagined a world without stores, any more than Kodak imagined a world where photos didn't require film and chemicals. So while Netflix plotted for a decade to make its world-class mail-distribution system irrelevant, Blockbuster clung to its stores and made itself irrelevant. It filed for bankruptcy protection in 2010.

Don't just play defense.

While many companies respond to technological change by clinging to their traditional markets and business models, Hasbro shows how an old-line business can claim new territory too. In the face of increasing competition from electronic games and entertainment, many of Hasbro's products seemed tired, and the market in which they were competing was in decline. Transformers—basically, robots that could disguise themselves as cars—were more than a quarter-century old. G.I. Joe went all the back to the early 1960s. But Hasbro invigorated sales by leveraging its brands beyond toys and games, for instance making them the basis for a series of big-budget Hollywood movies. Hasbro also effectively adapted Scrabble to modern technology. Rather than just fight a rearguard action and protect sales of Scrabble boards, Hasbro now lets people play Scrabble on smart phones and other mobile devices.

Make sure you look good naked.

Textbook publishers have traditionally been all bundled up. They relied on their lobbying with states to win the right to sell books, rather than having open, continual competition based on price, quality, or anything else.

The situation is beginning to change because of consumer uproar about the cost of college texts, budget cutbacks at schools, and reforms in the educational system. Now technology is poised to destroy the traditional textbook business model altogether, because the spread of electronic devices is reducing the need for books and creating an open field for innovation. Some smart publishers are starting to experiment with new ways of delivering their content that will look great naked—meaning it won't be wrapped in the traditional format of a book. They're doing it because costs will be reasonably low and because the benefits will be enormous. Basically, the textbook can become the electronic hub for educating a student.

Johnny won't just read a book on his tablet. He'll be able to tap into other resources

Four Principles for Crafting Your Innovation Strategy

right from his textbook, like teacher notes, videos, and tutors. When Johnny finishes his homework, the computer will correct it for him immediately and make suggestions about what to do differently. Parents will be notified that Johnny has done his homework (or not). The teacher will get an e-mail that night showing which problems caused problems for the class, so the teacher can address those the next day. School administrators will, over time, get information about which teachers are having success and which aren't. Textbook publishers will get data about areas that are confusing students and will be able to test different wording and different teaching methods.

Accelerated Turnover

Any list of the most successful companies in the U.S. would see about half of its members drop off every decade, and we're willing to bet that the turnover in the next 10 years will be even higher than that. Companies will have to adapt to a world in which they don't control the conversation with their customers. Customers will talk with each other, talk back to the company, talk to other companies, and on and on. Every permutation will be possible, and companies will struggle to innovate adaptations.

But as Schumpeter saw, every act of destruction provides an opportunity to create. Although seizing those opportunities will be tricky because it's hard to discern exactly how the future will look, we find ourselves turning back to one of the famous sayings of our old friend and colleague, computing pioneer Alan Kay. He says: "The best way to predict the future is to invent it."

Paul B. Carroll and Chunka Mui are co-founders and managing directors of Devil's Advocate Group, a consultancy that helps businesses test their innovation strategies. They are also co-authors of Billion-Dollar Lessons: What You Can Learn From the Most Inexcusable Business Failures of the Last 25 Years.

Social Surveillance Yields Smarter Directions

Social Surveillance Yields Smarter Directions

Phone app Waze uses real-time information shared by drivers to tweak its directions and traffic advice.

By Tom Simonite

Most drivers will be familiar with the feeling that trying a slightly different route, or leaving a few minutes later, would have saved them time in traffic, and some may have tweaked a familiar route to test the notion. A free navigation app for smart phones called **Waze** performs such experiments at a grand scale by treating its users as road-going data probes.

Waze users automatically broadcast their GPS position and speed to Waze over the Web at all times. Social-networking and gaming features built into the app also encourage them to actively share information such as the location of hazards and traffic jams. When a user asks the app for directions, those sources of information influence Waze's routing algorithm. Users can see the position and speed of other users on a map, and also receive live hazard reports. The data collected by the app is used to refine Waze's map in other ways, showing, for example, the location of unmapped streets.

"In the old world, you would flash your lights at someone. Now we can deliver the experience and intuition of other drivers to you through the app," says Noam Bardin, the company's CEO. Waze, which is based in Israel and Palo Alto, California, currently has more than 2.6 million users worldwide, roughly 800,000 of whom are in the U.S.

Waze awards points to drivers for miles driven with the app running, and also for submitting hazard reports. Making a report while driving, to indicate problems such as traffic jams, speed traps, or accidents, requires just three taps on the phone. Users can also create and join groups to follow reports from people who drive a particular route or area, or compete with friends to rack up the most points.

Those points do more than just make users feel good, says Di-Ann Eisnor, vice president and community geographer at Waze. "We use it as a confidence score for the contributions that user makes," says Eisnor. A report of a traffic jam from a low-ranked user is less likely to change the route suggested by Waze than one from a high-ranked user, for example.

Social features like that are what really set Waze apart, says **Alex Bayen**, a researcher at University of California, Berkeley, whose group previously developed **a phone app** that simply collects traffic data. "There are many sources of traffic information but no

Social Surveillance Yields Smarter Directions

other app lets you see other drivers around you and actively work together to post about traffic problems," he says.

Most GPS navigation devices and apps that advise on traffic do so based on a mixture of historical traffic patterns and input from sparsely distributed road sensors, says Eisnor. Google's free navigation app for Android phones combines users' GPS trails with more traditional sources, although it offers fewer features than Waze.

"Unlike other apps, Waze is used a lot even when people don't need to be told when to go, like for commuting," Eisnor says. About 70 percent of trips made with Waze do not involve asking it for directions. Instead people leave it running on their phone to see real time traffic data, receive warnings of hazards reported by others and contribute themselves to the community.

The southwest-Florida TV station [NBC-2](#) has created a Waze group for local commuters, and it now bases its reports exclusively on information and maps drawn from that community and other Waze users in the area. "They found that information from Waze was as good—and even better than—the paid-for traffic data they used before," says Eisnor.

To encourage users to probe conditions in uncharted areas and thus extend Waze's coverage, the company employs a game-like feature: icons dubbed "road goodies" placed on the map. Users earn points for driving over the virtual goodies, and often diverge from their route to do so, says Eisnor.

Mikel Maron, a developer and member of the board of [Open Street Map](#), a collaborative project working to build a free, editable online map of the globe, says he can understand why users might be willing to change their route to gather data that helps others. Some of the data collected by Open Street Map is used by Microsoft's Bing Maps service.

"I know that once people start mapping in Open Street Map, it becomes a kind of addiction. You really want to help fill in the white spaces," says Maron. "I imagine that is perhaps how someone would feel about helping others by improving Waze's coverage." However, he says some people may reconsider when it becomes clear that Waze seeks to make money using their data.

One revenue strategy under development at the company involves placing virtual coupons or discounts on the road for collection. "We're currently experimenting to see what influences behavior and find out what incentives work," says Eisnor. "We've been

Social Surveillance Yields Smarter Directions

surprised by what the threshold is." Waze's advertising platform launched in Israel two months ago. A recent trial in San Francisco awarded free concert tickets to the user who **drove over the most promotional goodies**.

Eisnor says that saving money can coexist alongside more altruistic motivations like helping to cut travel frustrations. "In time, I want to answer the question of whether we can reduce congestion based on coupons at Starbucks," she says.

Bayer says he thinks that advertising and fixing traffic jams could go together. "I think it would be possible in future to use personalized incentives to try and decongest freeways by altering drivers' routes," says Bayer, "the driver and promoter might get something out of it but there can also be a public good."

Copyright Technology Review 2011.

Can Social Networking Keep Kids in School?

Can Social Networking Keep Students In School?

by LARRY ABRAMSON

February 9, 2011

Last fall, students were psyched to be starting school at Coppin State University in Baltimore.

But if history is any guide, 40 percent of them will disappear before next year — victims of this school's low retention rate.

This is the time of year when students are wondering whether they will get accepted to the college of their choice. But many colleges and universities are asking themselves another question: How can we hold onto students once they're enrolled?

Some schools see half their freshmen disappear because so many drop out. To address this problem, some schools build physical spaces — new dorms with themes and clubs to make sure new students get involved. Those strategies can help.

But schools are now trying to keep students coming back with a new twist on a familiar tool — social networking.

A School-Based Facebook

The Bill and Melinda Gates Foundation has also been looking for new approaches to keep students coming back.

The foundation is announcing Wednesday that it will invest \$2 million in [Inigral](#) — a company that is trying to build virtual college communities by creating school-based Facebook sites. It's the first time that the Gates non-profit foundation has bought an actual equity stake in a for-profit company.

"What we do is make sure that when students arrive they either already have

Can Social Networking Keep Kids in School?

assembled or [can] very quickly assemble that kind of peer support," says Michael Staton, the CEO of Inigral.

Peer support means a ready network of friends. Only students can gain entry to these sites, and they're invited in the moment they are accepted to a school. The feel is supposed to be small and intimate, unlike school's fan sites on Facebook, which are open to everyone, and don't inspire much networking.

Merging Social And Academic Lives

Columbia College, an arts and media school in Chicago, has been experimenting with the site. Samantha Saiyazonsa, a sophomore in journalism, says it helps her merge her social and academic lives.

School clubs can also use this technology to recruit and discuss campus issues. The sites are there for students, not for administrators.

Schools pay what they say is a nominal fee for Inigral to build the site. Colleges and universities hope that they will get paid back through greater student engagement, and higher retention rates. Ultimately, that saves schools money because they don't have to replace all those dropouts.

"We have some indication that first-time freshmen who opted to participate in the application were highly more likely to be retained for the next semester," says Kari Barlow, an online administrator who spearheaded Arizona State University's experiment with Inigral's [Schools App](#).

Hard To Measure The Impact

It will be tough to show whether these efforts played any direct role in students' decision to stay or go — that's a subject for future research. And, of course, many students are out of reach for this and other approaches.

Can Social Networking Keep Kids in School?

Alexis Thompson, a sophomore who uses Columbia College's site, says it only works if kids work with it.

"That's something that they have to be proactive about," she says. "So, the Facebook app can be there. But unless you're being proactive and you want to go out and look for things like that — it's really on the student."

The Gates Foundation investment seems to show that the organization is casting a wide net to find new ideas that will improve outcomes in higher education.

A Year Later, Microsoft Picture Looks Very Different

A year later, Microsoft picture looks very different

By Bill Rigby

SEATTLE | Tue Jan 25, 2011 9:21pm EST

(Reuters) - A year ago, Microsoft Corp blew away Wall Street's earnings forecasts with blistering sales of its new Windows 7 operating system and trumpeted optimism about the recovery in tech spending.

This week, with its stock trading slightly lower than a year ago, the world's largest software company is set to report lower profit as PC sales growth fizzles, and it struggles to convince investors that it can grab a foothold in the fast-moving mobile and tablet markets.

"Microsoft is still a juggernaut in the PC business, Windows-based machines are still selling over 300 million a year," said Tim Bajarin, president of tech research firm Creative Strategies.

"But they missed the smartphone revolution, and even though they were the first to really push the tablet, Apple basically redesigned it and left Microsoft in the dust."

Most investors expect a solid quarter for the company, but are more focused on fears that Microsoft's new Windows phone software isn't selling well. And while approving of a recent decision to make a version of Windows for ARM chips, the market realizes that means there won't be a Windows-based challenger to Apple Inc's iPad for at least two years.

"I wish they did this (the switch to ARM) two years ago, it's something they should have thought of," said Sid Parakh, analyst at McAdams Wright Ragen. "But it is a long game. The question becomes: Is the iPad a cannibalization of Microsoft's existing products, or

A Year Later, Microsoft Picture Looks Very Different

an added component of consumer electronics spending? I'm sure it's a mix of both."

SOLID QUARTER, NO FIREWORKS

PC sales, the surest guide to Microsoft's overall health, rose only 3.1 percent in the last three months of last year, according to research firm Gartner. The year as a whole didn't match early optimism, with PC sales rising 13.8 percent, well below Gartner's summer forecast of 19.2 percent.

The good news for Microsoft is that business customers -- the core market for its software -- are buying new computers more readily than cash-strapped consumers, who are holding off on purchases or buying iPads instead.

The resilience of business customers helped tech bellwethers IBM and Intel Corp post positive results and outlooks over the past two weeks, helping their stocks higher.

But the market likely will demand more from Microsoft.

"We're investors, we have short memories," said Kim Caughey Forrest, senior analyst at Fort Pitt Capital. "We need a lot of reassurance."

Microsoft is expected to report profit of 68 cents per share, according to Thomson Reuters I/B/E/S, lower than the 74 cents it reported a year ago.

Sales of Windows 7 are still going strong, but likely won't match the year-ago figure, which was boosted by a one-time deferral of revenue from pre-sales of the operating system.

Overall sales are expected to inch up to \$19.2 billion from \$19 billion a year ago, helped by the unexpectedly strong sales of the Kinect hands-free gaming system, which sold 8 million units over the holiday shopping season, above Microsoft's own target of 5 million.

A Year Later, Microsoft Picture Looks Very Different

However, given the generally lower profit margins on hardware as opposed to software, the Kinect sales are not expected to trigger a spike in profit.

APPLE CRUISES PAST

One uncomfortable fact for Microsoft: unless it posts blowout numbers, it will have lower quarterly profit than Apple for the first time in recent memory. The last time Apple produced more profit in a year than Microsoft was 1990.

Last week, Apple announced a record \$6 billion quarterly profit on strong-selling iPhones and iPads over the holiday shopping season. Analysts expect Microsoft to post profit of \$5.93 billion for the same quarter. Two years ago, Microsoft's profit was almost double Apple's.

It could be a painful moment for Microsoft, which effectively saved Apple from extinction with a \$150 million investment in 1997.

"It's psychological," said Parakh. "There's no doubt Apple has momentum, they've built great products that people want to buy. It's another indication of the challenges facing Microsoft."

Apple roared past Microsoft in market value last May, and overtook it in terms of revenue in the quarter ended last September. Apple now has a market value of \$311 billion -- second only to oil giant Exxon Mobil Corp in the Standard & Poor's 500 index -- and well ahead of Microsoft's \$243 billion.

If the company does not impress Wall Street this quarter, or show it has a realistic plan for growth, questions will be asked about the leadership of Steve Ballmer, now in his 12th year as chief executive.

A string of high-level departures has raised concerns about his efforts to revitalize the

A Year Later, Microsoft Picture Looks Very Different

company.

Ballmer "is always on thin ice," said Forrest at Fort Pitt Capital. "Microsoft is a results-driven company."

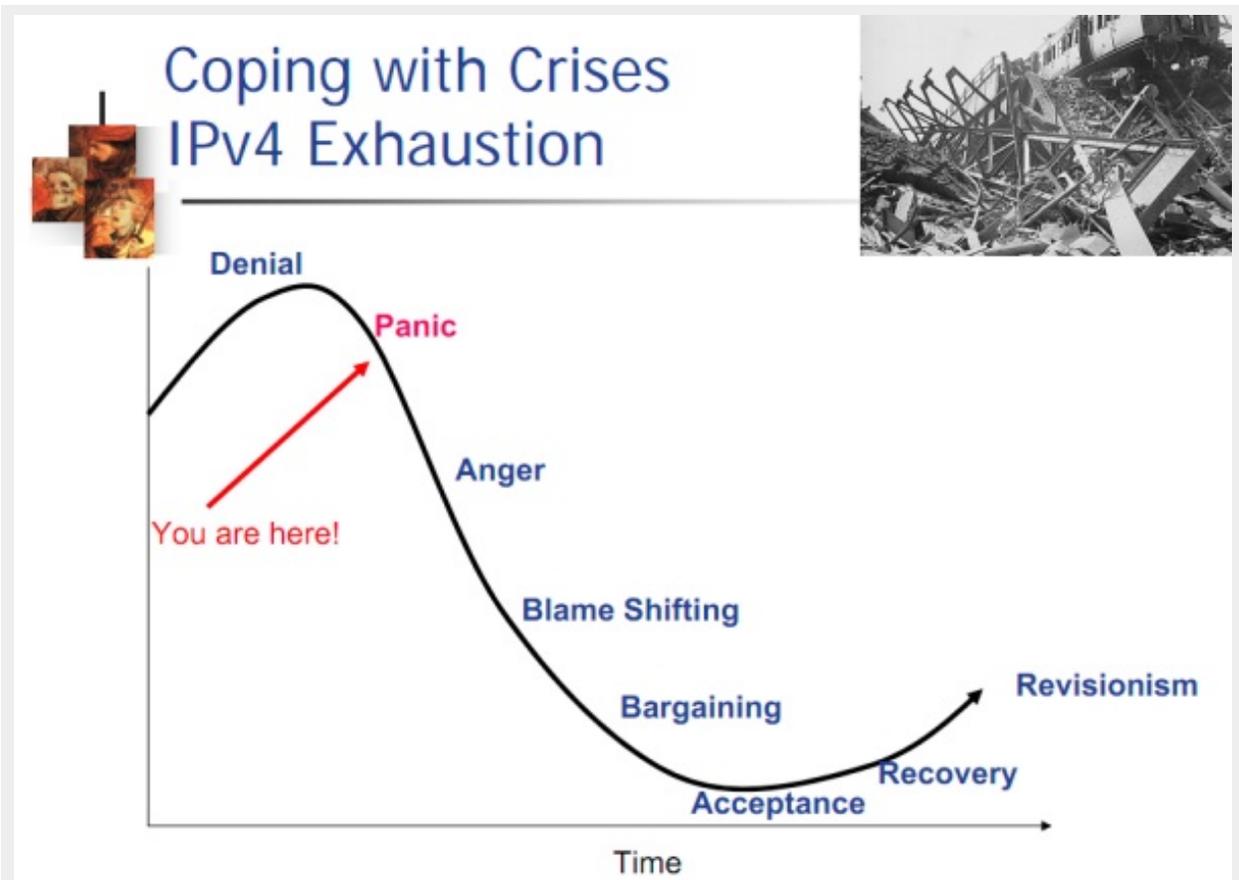
(Reporting by Bill Rigby; Editing by [Bernard Orr](#))

Why the Entire Internet Is about to Become 'Slower and Flakier'

Why the Entire Internet Is about to Become 'Slower and Flakier'

We've failed to transition to new technologies, and we've exhausted available Internet addresses.

CHRISTOPHER MIMS 01/23/2011



Slide from a presentation on the exhaustion of the supply of addresses for devices on the internet ([pdf](#)) by Geoff Huston, Adjunct Research Fellow at the Centre for Advanced Internet Architectures

Seven days from today, according to ISP Hurricane Electric, the organization that gives out the unique 9-digit addresses that in theory identify every device connected to the Internet is going to simply run out of those addresses. (This is only an estimate; Japanese ISP iNetCore [pegs the end to 2 days later.](#))

Why the Entire Internet Is about to Become 'Slower and Flakier'

It's as if the local telephone company simply ran out of phone numbers to give to its customers. Except every time this happened, back when everyone had a land line and area codes meant something, the telephone company saw it a mile away, and added a new area code for a given geographic area, thus averting catastrophe.

In this case, **there is no plan B**. Years -- decades, really -- of foot-dragging mean that the world's hardware manufacturers, OS coders, website builders and Internet service providers are stuck with the existing system. When the last block of IP addresses, as they're known, is handed out, that's it.

Does this mean no more computers can be connected to the Internet after January 31st, 2011? No, of course not - if you're Apple, HP, Xerox, Ford or one of the other companies that got a gigantic block of IP addresses in the early days of the Internet, you'll hardly notice; these companies are using only a fraction of the IP addresses they reserved all those years ago.

Everyone else, the rabble drawing from the well of free IP addresses that's about to run dry, has problems that will slowly grow worse. At first, your Internet Service Provider is going to solve the problem for you, possibly by **buying more IP addresses for what are likely to be ever higher prices** as the gap between demand and supply widens. What's mostly likely, though, is that your ISP is going to implement a kludge: they'll use something called **Network Address Translation** (NAT) to hide more and more users under one of the IP addresses they already possess.

In other words, you're going to start sharing a phone number with a stranger. If they misbehave and are banned, you'll be banned as well. That's unlikely, but here's what's almost assured: slowly, our experience of the Internet will start to degrade. If we're lucky, the change will remain imperceptible, and if we're not, well...

As Google engineer Lorenzo Colitti recently **told Agency France Presse**:

"You will start to share with your neighbors, and that causes problems because

Why the Entire Internet Is about to Become 'Slower and Flakier'

applications can't distinguish you apart," Colitti said. "If your neighbor ends up in a blacklist, you will too."

"The Internet won't stop working; it will just slowly degrade," he continued, explaining that systems would eventually have trouble handling multiple connections on shared addresses. "Things will get slower and flakier."

Though NAT has been in use for a long time, most applications are tuned to pass their data through only a single layer of NAT. And that single layer is almost certainly already in use -- NAT is the reason that every device in your house connected to your WiFi base station appears, to the Internet at large, to have the same IP address.

What happens when your BitTorrent client or your Skype or other VoIP application starts communicating through more layers of NAT, which works by shunting data through other ports, some of them less desirable, is that things break down.

Generally, the Internet is OK with that -- packets of data can be re-sent when they fail to arrive -- but at the cost of speed.

It's not as if the Internet is going to break in a week. The correct analogy is rot - in a week, the shipworms are unleashed, and the planks that stand between you and the briny depths of an unusable connection to the most important communications network on the planet begin to be compromised by a potentially endless series of imperfect hacks designed to postpone the inevitable.

The inevitable, of course, is an upgrade from the current Internet communications protocol, IPv4, to the **next-generation standard, IPv6**. The problem with that inevitability is that the price of switching to IPv6 is going to be so high - in terms of reliability, backwards-compatibility, actual money and a hundred other potential issues, that before the bulk of the users of the Internet are finally forced to switch to IPv6, the existing IPv4 network will probably have to degrade to some extent.

Speculation on how bad things will get before that happens is pointless -- it's a

Why the Entire Internet Is about to Become 'Slower and Flakier'

question of switching every device in the world over to a new protocol; in essence, an economics question. And we all know the value of predictions in that realm.

To Avert Internet Crisis, the IPv6 Scramble Begins

To avert Internet crisis, the IPv6 scramble begins
by [Stephen Shankland](#)

Remember Y2K? The Internet today is facing a similarly big problem all over again, but nobody knew exactly when it would hit--until now.

The problem is the day the conventional Internet runs out of room for new computers because the world has used up the supply of Internet addresses that computers need to communicate over the Net.

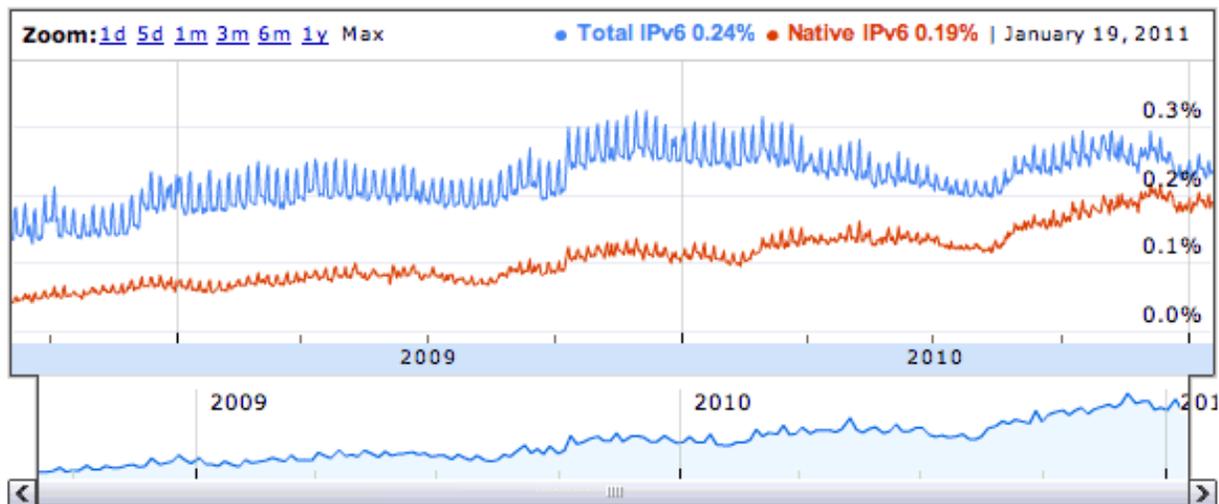
It's likely that this week or next, the central supplier of Internet Protocol version 4 (IPv4) addresses will dole out the last ones at the wholesale level. That will set the clock ticking for the moment in coming months when those addresses will all be snapped by corporate Web sites, [Internet service providers](#), or other eventual owners.

And that means it's now a necessity, not a luxury, to rebuild the Net on a more modern foundation called IPv6.

It's taken a long time because there was little immediate payback for companies spending money and time to build IPv6 support. But even though the carrot to motivate people has been pretty small, the stick now is getting bigger with each passing week.

"Many are waiting for a 'killer application' for IPv6. This is a misconception," said Lorenzo Colitti, the Google engineer overseeing the search giant's years-long transition to IPv6, in a 2010 talk.

"The killer application of IPv6 is the survival of the open Internet as we know it."



Only a tiny fraction of Google users--about 0.2 percent--are equipped to use the next-generation IPv6 technology that will relieve growth pressures on the Internet.

(Credit: Google)

Minimizing disruptions

To Avert Internet Crisis, the IPv6 Scramble Begins

Many expect some disruptions as the IPv6 shift takes place. Web sites could be slow or inaccessible, companies could have a harder time setting up new services, Internet service providers could have a hard time keeping up with subscriber growth, and security will have to adapt to the new technology.

The Net won't collapse, though.

Leslie Daigle, chief technology officer of the [Internet Society](#), a standards and advocacy group, likens the situation to a changing separation of railroad tracks. Trains for one can't travel on tracks for the other, and moving data between the networks is, in effect, as onerous as unloading and reloading train cars' cargo.

"If you have a Web site, you are basically going to have some customers coming on wide gauge and on narrow gauge," Daigle said. "Narrow gauge is going away."

To give the world a chance to wrestle the IPv6 bull directly by the horns, the Internet Society is helping to organize the [World IPv6 Day](#). On June 8, content providers such as Google and Yahoo and content distributors such as Akamai and Limelight Networks will offer their services over IPv6 for 24 hours for a collective evaluation and troubleshooting session.

That means, for example, that Google will enable IPv6 service on its primary domains, not just in a dedicated corner such as today's [ipv6.google.com](#) (that link won't work for most folks today). Those with IPv6 connectivity will help to stress test a tender new Internet.

People who want to get an earlier start can point their browser to an [IPv6 readiness test page](#) to see how far along they are. All modern personal computer operating systems can handle IPv6 with no trouble, but the connection to the Internet is another question entirely.

The end in sight--for years

Experts have known for ages that the limit of 4.3 billion IP addresses would be a problem with the prevailing Internet Protocol version 4. The problem stemmed from a 1977 decision by Vint Cerf, who now is an Internet evangelist at Google.

At the time, just a few years into the Internet's history, he decided to use 32-bit Internet addresses. But 2 to the 32nd power, about 4.3 billion, looks a lot smaller in 2011 than in 1977.

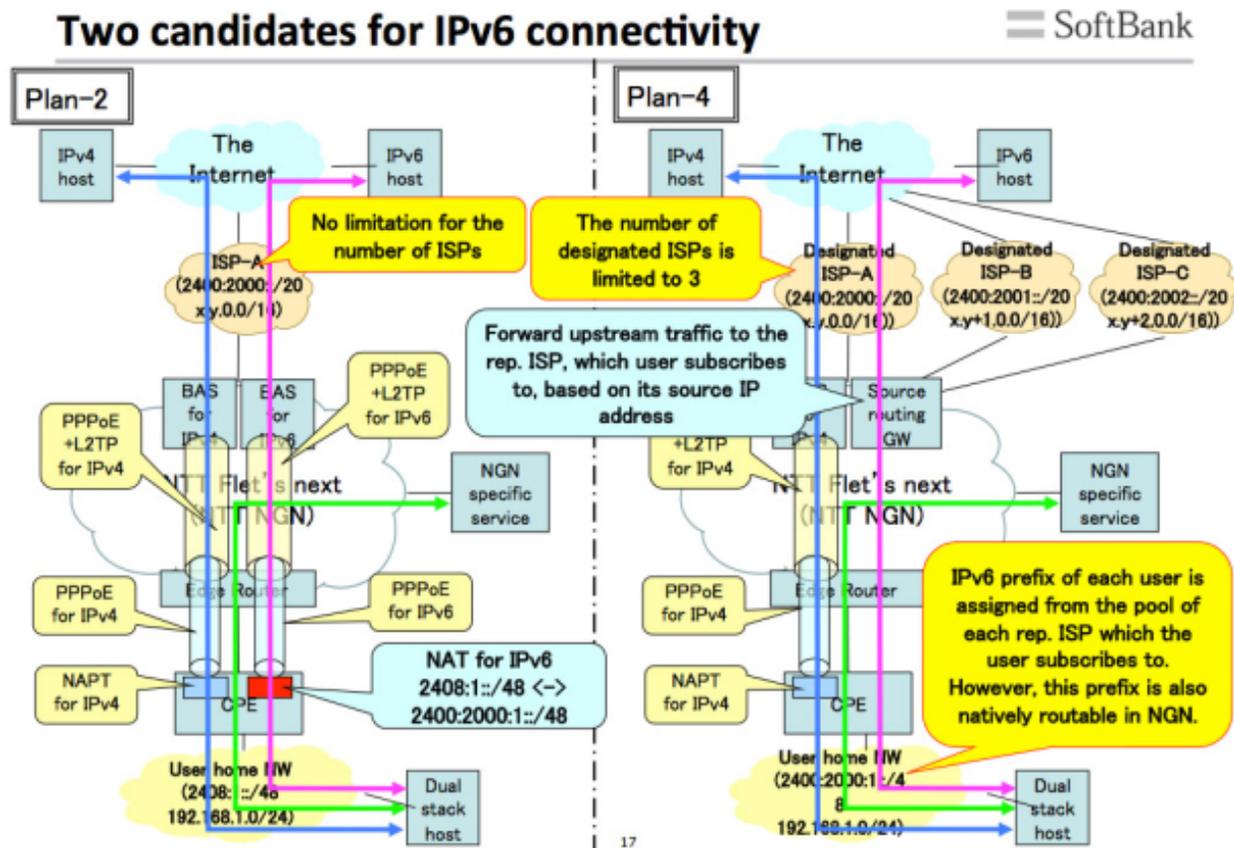
"Who the hell knew how much address space we needed?" [Cerf told journalists](#) in Sydney, Australia, recently.

It didn't take until today to figure out an answer to that question, though. That's why in the 1990s, Internet engineers developed IPv6, which has a practically inexhaustible supply. To be precise, [340,282,366,920,938,463,374,607,431,768,211,456](#) addresses.

The big problem, though: IPv6 isn't compatible with IPv4, so making the transition is painful for a wide spectrum of the computing industry.

To Avert Internet Crisis, the IPv6 Scramble Begins

The [Internet Assigned Numbers Authority](#), which doles out IPv4 addresses in blocks of 16.8 million called slash-eights or /8s to five organizations called regional Internet registries (RIRs), only has seven of the 256 "slash-8" blocks original 256 /8s left. And after the next two are handed out, the remaining five will automatically be distributed to each of the RIRs, which in turn will offer them to Internet service providers, hosting companies, and others with an appetite.



Yahoo Japan's broadband service has been evaluating the best ways to offer IPv6 connections. It's not simple.

(Credit: Yahoo Japan/Softbank)

The imminent exhaustion of IANA's IPv4 addresses helps put a timetable on the IPv6 transition. That's a big change from the last decade, when IPv4 exhaustion was clearly going to happen but not on some specific schedule.

Setting a deadline

The timing is helpful for getting planning in gear. In fact, it makes the IPv6 transition look more like Y2K, the expensive problem that peaked on January 1, 2000, when computers storing dates with only two digits could confuse 2000 with 1900. Like Y2K, the IPv6 transition requires companies to spend money on mundane infrastructure upgrades rather than exciting new revenue-

To Avert Internet Crisis, the IPv6 Scramble Begins

generating services.

But there's a big difference between the Y2K and IPv6 challenges. Y2K was mostly limited to isolated computing systems. With the exhaustion of IPv4 Internet addresses, the entire Internet needs to be upgraded to IPv6--everything from Web sites to smartphones, from networked gaming consoles to routers that pass information across the Internet.

That means regular folks are going to be dragged into the IPv6 transition, said Martin Levy, director of IPv6 strategy at [Hurricane Electric](#), a back-end Internet service provider that has had a concentrated IPv6 program for years.

"When you walk into [electronics stores such as] Fry's, Dickson's, or Comet, you look at the shelves and pick the wireless gateway you want for your home. You may want 802.11n or a printer port or storage," Levy said. "But at what point do you say, 'I want v6 enabled'? You don't have a realization as a consumer that this is important."

And as with Y2K, when companies bought a glut of new servers to replace aging systems, there's money to be made from the IPv6 transition. Hurricane Electric isn't the only one with a sales pitch.

[NTT America](#) has had a specialized service for helping companies through the change. And AT&T, which "has invested millions of dollars to ensure that its own network and services are ready to make the transition to the new Internet Protocol," yesterday announced a consulting service for businesses facing the change.

Early adopters

Not everyone is scrambling, though. Google is perhaps the best example of a company that's been working to [adjust to IPv6 before crunch time](#). It's used IPv6 both for internal operations and, increasingly, external sites.

In 2008 came Google search over IPv6, with a public launch in January 2009. In March 2009 came Google Maps, then in August the first IPv6-enabled Android phones. In February 2010, YouTube showed up, leading to an overnight surge in Google's outgoing IPv6 traffic.

"The key lesson that we learned was starting early and taking the transition slowly. It was cheap and relatively easy," Colitti told CNET. "We also found that an incremental approach was key: by bringing IPv6 to one service at a time and using shim layers when communicating with back-ends, it's possible to achieve slow but steady progress rather than have to tackle the whole code base at once. Unfortunately, it's getting late for that approach now."

Facebook, too, has been working on the problem, and like Google, has been avoiding the idea of separate internal infrastructure for IPv4 and IPv6.

"Since last summer, we've offered Facebook over IPv6 at www.v6.facebook.com," said Donn Lee, a Facebook network engineer. We leverage as much of the existing systems in our data centers to minimize separate paths and functions for v6. We are not unique in this practice. Others are following similar strategies. Having a parallel Facebook for v6 won't scale."

To Avert Internet Crisis, the IPv6 Scramble Begins

Where's the appetite for IPv6 data? A huge amount, at least for Google in 2010, was France. That's because, [Free.fr](#), a French Internet service provider that offers phone and TV service as well, made the jump to IPv6 in 2008.

They're still a rarity. [Google statistics](#) show that a little over 0.2 percent of Google visitors today would get Google services over IPv6 if they were offered on the company's primary domains rather than IPv6-specific addresses.

Unfortunately for early adopters, there can be an IPv6 penalty. IPv6 routes across the Internet can meander through distant, sometimes overloaded gateways rather than connect computers more directly, Yahoo IPv6 expert Jason Fesler said in a presentation last year. "A small percentage of the users will, when given the chance to connect to an IPv6 address, time out instead of quickly and transparently failing over to IPv4," he said.

In other words, at times, IPv6 servers will appear to be offline--something that makes Yahoo "a bit timid" about serving content over IPv6. It lags Google and Facebook, in part because of higher priority engineering projects, and plans to begin offering its services over IPv6 in late 2011, Fesler said.

That's changing, though. Gradually, nodes on the Internet will start getting wired into the IPv6 Internet, relieving congestion. Right now, by Hurricane Electric's measurements, [8 percent of those nodes are on IPv6](#).

"More and more networks are going v6; but that's a measurement in the core of the networks, not the end user connections," Levy said. "We see that improving day over day."

Worth it in the end

Perhaps the best news about the IPv6 transition is that, once it's mostly over, the Internet will be a qualitatively different place. With vast tracts of IP addresses available, individual ones can be assigned to phones, computers, cars, stereo components, living-room thermostats, heads-up display glasses, wristwatches, home solar panels--you name it. Where a case can be made for networking, these devices will be able to communicate directly without the network topology shenanigans such as network address translation necessary today.

One consequence of that more direct connection is the elevation of peer-to-peer communications in the network. Central servers will remain important, but no longer necessarily a gateway.

Less revolutionary but probably more persuasive for those in the computing trenches, IPv6 makes the more mundane business of networking easier, too. There, perhaps, people can relish a little taste of the carrot even as they smart from the stick .

"Direct connections between users and sites...allows for faster, more reliable, more secure, and less costly Internet service," Facebook's Lee said. "Almost everyone in the Internet ecosystem is motivated along these lines."

Drumming Up for Addresses on the Internet

Drumming Up More Addresses on the Internet

By LAURIE J. FLYNN

Who could have guessed that 4.3 billion Internet connections wouldn't be enough?

Certainly not Vint Cerf.

In 1976, Mr. Cerf and his colleagues in the R.& D. office of the Defense Department had to make a judgment call: how much network address space should they allocate to an experiment connecting computers in an advanced data network?

They debated the question for more than a year. Finally, with a deadline looming, Mr. Cerf decided on a number — 4.3 billion separate network addresses, each one representing a connected device — that seemed to provide more room to grow than his experiment would ever require, far more, in fact, than he could ever imagine needing. And so he was comfortable rejecting the even larger number of addresses that some on his team had argued for.

“It was 1977,” Mr. Cerf said, in an interview last week. “We thought we were doing an experiment.”

“The problem was, the experiment never ended,” added Mr. Cerf, who is a former chairman of the [Internet Corporation for Assigned Names and Numbers](#), or [Icann](#), a nonprofit corporation that coordinates the Internet naming system. “We had no idea it would turn into the world's global communications network.”

Today, the Internet that Mr. Cerf helped create more than 30 years ago is about to max out. Within the next 12 to 18 months, or perhaps sooner, every one of the 4.3 billion

Drumming Up for Addresses on the Internet

Internet Protocol addresses will have been allocated, and the Internet, at least as it exists today, will have reached full capacity.

I.P. addresses are the unique sequence of numbers assigned to each Web site, computer, game console or smartphone connected to the Internet. They are distinct from domain names, which identify Web sites, like nytimes.com.

“There are 4.3 billion addresses, and a lot of people have more than one,” said Leo Vegoda, manager of number resources at Ican. “And there are seven billion people on the planet. That’s a big mismatch.”

The rapid expansion of Internet adoption in Asia has sped things up even more.

Experts saw this problem coming years ago, and the transition to a new system, referred to as Internet Protocol version 6, is well under way. This new standard will support a virtually inexhaustible number of devices, experts say. But there is some cause for concern because the two systems are largely incompatible, and as the transition takes place, the potential for breakdowns is enormous.

“This is a major turning point in the ongoing development of the Internet,” Rod Beckstrom, Ican’s president and chief executive, said. “No one was caught off guard by this.”

Still, the question looms, is the Internet industry prepared?

The answer depends on whom you ask. While it is true that no one has been caught off guard, some parts of the industry responded faster than others, leaving some technology

Drumming Up for Addresses on the Internet

companies scrambling to catch up. Software companies like [Google](#), [Microsoft](#) and [Facebook](#), along with PC makers, say they have been taking the problem seriously for years in hopes of thwarting any major calamities. The major operating systems — like Microsoft's Windows 7 and [Apple's](#) Mac OS X — have already incorporated the new system. And providers, including [Comcast](#), say they are ready to make the switch.

But Mr. Cerf is critical of Internet service providers, along with the manufacturers of Internet devices, for not addressing the problem sooner, saying that many chose to wait until customers started asking for the new system.

“How can customers be expected to know what they need?” Mr. Cerf said. He compared Internet protocols to the internal workings of a car engine. “It’s like changing a gear in a car’s transmission,” he said. “People shouldn’t have to worry about that.”

I.P. addresses are allocated by the Internet Assigned Numbers Authority, which is operated by Iann, to five registries representing regions of the globe. Those registries distribute the addresses to Internet service providers like cable and phone companies, universities, governments and large corporations. Millions of new devices will be attached.

At a ceremony early this month in Florida, the last block of addresses based on the original standard, known as IPv4, were allocated to the five registries.

Comcast began working on the problem nearly six years ago, and last year began customer trials nationwide. Jorge Alberni, a Comcast spokesman, said the trials so far had gone smoothly.

Drumming Up for Addresses on the Internet

Comcast is now beginning to distribute dual-mode cable modems, for example, that support both the original and the new Internet Protocol versions. By the time the transition is fully under way, Mr. Alberni said, most Comcast customers will already be using cable boxes and modems that support IPv6, as the new version is commonly called. In some case, customers with older equipment will have to make a swap.

“We don’t foresee any problems for our customers,” he said.

To help make the transition to IPv6 easier, [Yahoo](#), Google and Facebook, whose Web sites generate a combined traffic of more than a billion visits a day, have agreed to participate in a sort of trial run on June 8, named World IPv6 Day, to make sure their systems are ready. Participants are hoping that such an experiment will shed light on potential glitches.

Still, Leslie Daigle, chief Internet technology officer at the Internet Society, a nonprofit Internet policy organization overseeing the test run, warned that the transition to IPv6 was complex, and would most likely cause headaches for customers as they grappled with compatibility problems. The hope is that the test run will reveal the exact scope of the challenge.

The change will require companies to retrain technicians and instruct help desk personnel how to field compatibility questions.

“I almost wish we could train the [Boy Scouts](#) and [Girl Scouts](#) to come to people’s houses to help out with this,” said Mr. Cerf, now chief Internet evangelist at Google. “This is not just about adding extra numbers,” he said. “It’s a different system.”

Drumming Up for Addresses on the Internet

If the transition is not done right and done quickly, he said, Internet users with new equipment could face problems viewing Web sites based on the original standard.

Mr. Cerf compares the size of the challenge to the problem facing computer users at the turn of the 21st century, when every software program out there had to be modified to recognize the year 2000 and beyond.

“We had to find every place on the network,” he said.

In the end, the year 2000 issue, often referred to as Y2K, caused very few interruptions. But in this case, the problem won’t go away after a certain date.

Mr. Vegoda is optimistic that most people will not notice the difference between the two standards, and expects the transition to go relatively smoothly. “Most Internet users have no idea they’re using IPv4 today and if things go well they will have no idea they’re using IPv6 in the future,” he said.

This article has been revised to reflect the following correction:

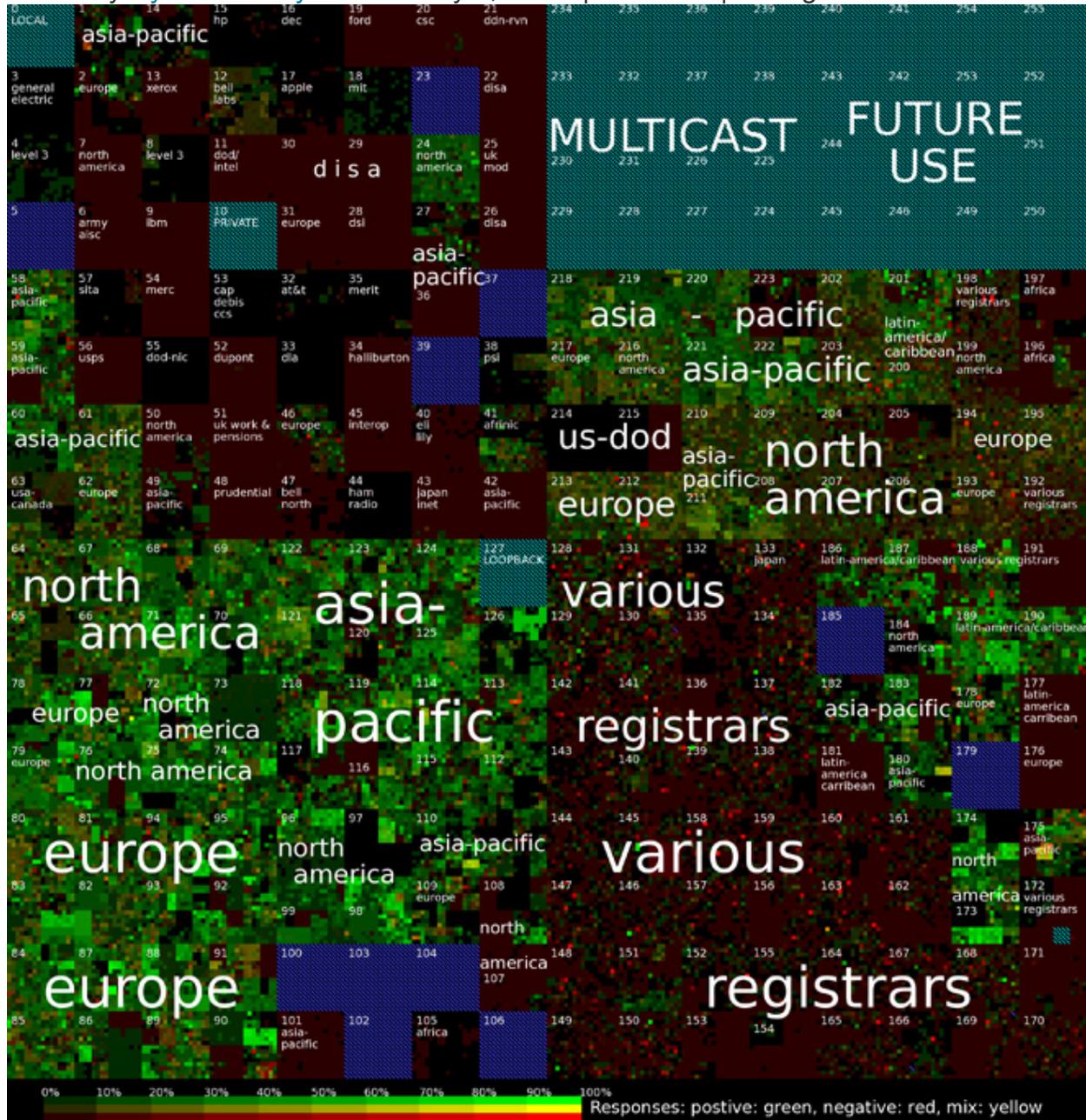
Correction: February 14, 2011

Because of an editing error, a previous version of this story misstated Vint Cerf’s relationship with the Internet Corporation for Assigned Names and Numbers, or Iann. He is a former chairman, not the current chairman.

No Easy Fix as Internet Runs Out of Addresses

No Easy Fixes as Internet Runs Out of Addresses

• By [Dylan Tweney](#)  February 3, 2011 | 9:58 am | Categories: [Broadband](#)



This map shows how much of the internet's address space is actually being used. But as of Thursday, the whole map has been allocated. *Courtesy USC/Information Sciences Institute*

No Easy Fix as Internet Runs Out of Addresses

The internet has run out of room.

Like a prairie with no more vacant land to homestead or a hip area code with no more cellphone numbers, the pool of available numeric internet addresses has been [completely allocated as of Thursday](#) (.pdf).

With that, the frontier has closed. The internet — in its current form — is now completely colonized. All that's left is to divide the allocated properties into ever-smaller portions, or to start trading what's already been assigned.

This change will have no immediate effect on ordinary people, but will eventually force any company that wants to be on the internet to reckon with a complicated and potentially expensive technology transition.

It could also introduce widespread delays and other strange behavior into the internet at large.

'It'll be harder to do things that used to be easy.'

"In a sense the net's going to get stickier," says John Heidemann, a computer scientist at the University of Southern California who has [done a survey of the distribution of internet addresses](#) (shown above). "It'll be harder to do things that used to be easy."

The shortage of addresses could eventually slow down your favorite web services, make it harder for websites to verify your identity, and complicate the design of services that depend on computer-to-computer connections, like peer-to-peer file sharing, Skype and more.

The change is going to happen gradually, over a period of years, but it will happen,

No Easy Fix as Internet Runs Out of Addresses

say experts who have studied the problem, and it starts today.

“This is 100 percent a real issue,” says Martin J. Levy, director of IPv6 strategy at Hurricane Electric, a provider of high-bandwidth data and collocation services that has been [predicting the exhaustion of addresses](#) for some time now. “We are dealing with a finite resource. We are going to run out. And we are going to have build a new system that gets around that issue.”

“It’s not really a shortage so much as exhaustion. It’s gone,” Kumar Reddy, a director of technical marketing at Cisco, says about the address space.

How Things Work Now

The data-delivery scheme used by the vast majority of the net, known as Internet Protocol version 4, uses a series of four numbers (each ranging from 0 to 255) to uniquely identify every machine that’s directly connected to the internet. That gives a total of about 4 billion possible IP addresses. These numbers, such as 63.84.95.56, underlie the more user-friendly domain name system, which uses URLs like www.wired.com.

IP addresses are like telephone digits, in that there’s a finite number of them. Unlike the telephone system, however, there’s no equivalent to the 718 or 346 area codes to expand to when Manhattan’s 212 is full. It’s as if every possible area code from 001 to 999 had already been utilized or reserved.

In some cases those “area codes” are full of paying customers. In other cases the numbers are simply being held for future use or reserved for technical reasons. But the bottom line is no new addresses are available.

It will take a while for the effects to trickle down to your level.

No Easy Fix as Internet Runs Out of Addresses

The organization responsible for allocating these numbers is the Internet Assigned Numbers Authority, which delegates blocks of IP addresses to five regional registries. It is IANA that allocated its last available IP address blocks to the regional authorities on Thursday.

The regional registries, in turn, allocate their IP addresses to companies, ISPs and telcos. With no new blocks coming from IANA, they will start to run out of their address pools over the next several years, starting with the Asia-Pacific authority, known as APNIC, probably in [mid-2011](#).

As regional authorities run out of available IP addresses, their clients will too. That means ISPs and companies will have difficulty assigning unique IP addresses to their customers, employees and servers as soon as this year, starting in Asia.

When that happens, those companies have a choice. They can switch to the next generation of the Internet Protocol, known as IPv6, which has 2^{128} available addresses. That's enough to give [5×10²⁸ addresses to every human being on Earth](#) — no danger of running out of addresses there.

The Problem With the Solution

But many popular sites, such as Wired's website, don't yet have IPv6 capability. In fact, less than 0.25 percent of the internet is wired to work with IPv6, which means that if you're using IPv6, there's not a lot of web content to browse.

Supporting IPv6 also means buying or upgrading network equipment, an expense most companies will want to avoid as long as possible.

So even though your [computer probably supports IPv6](#), your [iPhone supports it](#), and your [ISP may even offer IPv6 service](#), it's of no use to you unless each machine

No Easy Fix as Internet Runs Out of Addresses

between your computer and the server that you want to reach is also using IPv6.

“There’s a lot of good stuff going on in this space, but it isn’t quite complete yet,” says Levy.

Workarounds

The alternative for companies is to implement workarounds, like network address translation (NAT), which lets multiple people or computers share the same IP address. It’s a technique that your home Wi-Fi router probably uses already, and it works fine — except that it makes certain kinds of computer-to-computer connections more difficult.

‘You can’t just rip and replace. You have to maintain some of that legacy connectivity.’

For instance, if you want to view a home webcam from your desktop at work, and you’ve got NAT at home, you can’t simply use the camera’s IP address. You need another system to coordinate the connection, and those additional systems add complexity.

There may be ways for companies to use the already-allocated addresses better. Heidemann surveyed all 3.5 billion allocated IP addresses, and got responses from only about 7.6 percent. Even accounting for technical difficulties or deliberately inaccessible sites, there are clearly a lot of unused addresses out there.

“There is some amount of headroom here. We can probably use the address space better,” says Heidemann. “However, with that is going to come higher management overhead.”

In addition to NAT, there are ways to translate IPv4 addresses to IPv6, helping to bridge the two kinds of networks. But eventually, everyone will be forced to adopt “dual-stack” solutions, where computers — from smartphones and PCs to web servers and e-mail servers — first attempt to connect using IPv6, then switch to IPv4 if that

No Easy Fix as Internet Runs Out of Addresses

doesn't work.

“Everything you do, probably for the next two decades, will be dual-stack,” says Joel Conover, senior manager for IPv6 at Cisco. “You can't just rip and replace. You have to maintain some of that legacy connectivity.”

In other words, anyone with a network to manage will be facing a combination of NAT and IPv4-to-IPv6 translation issues, as well as the difficulty of managing dual-stack systems for some time to come. This will increase the complexity and cost of internet services, and there are bound to be some bumps along the way.

That's why, even though IPv6 has been available for about 10 years, it still hasn't been widely deployed. People are putting it off as long as they can. Now, with the pool of IPv4 addresses running out, the stalling tactics are finally going to stop working.

To help make the transition smoother, companies such as Google, Facebook and Cisco are planning to participate in “[World IPv6 Day](#)” later this year.

It's intended to be a chance for companies to set up and test IPv6-compatible systems, in the hopes that if they build the field, someone will come to play on it eventually.

“The companies that are going to be the most aggressive in implementing IPv6 are the ones that are the most-concerned about your experience on their website,” says Conover.

Remember that the next time you have trouble connecting to your home-security webcam. It might just be the shortage of IP addresses that's at the root of your trouble.

US Puts End to India Export Restrictions

U.S. Puts End to India Export Restrictions

By SHAUN TANDON, AGENCE FRANCE-PRESSE

Published: 25 Jan 2011 23:43

WASHINGTON - The United States on Jan. 25 said it was ending export restrictions for India's defense and space industries, eyeing trade with a nation shunned for more than a decade over its nuclear weapons program.

President Obama's administration also said it would welcome India into the club of nations that regulate export controls, bringing New Delhi full circle from an outcast to a member of international weapons controls.

The United States took major groups off a blacklist, including the Indian Space Research Organization, which leads India's space program, and the weapon-designing Defense Research and Development Organization.

Previously, the United States barred exports to the organizations of material and technology that could have military use.

"These actions will open important new opportunities for our companies and governments on cooperating in the defense and space areas," said Robert Blake, the assistant secretary of state for South Asia.

Blake, speaking Jan. 25 at Syracuse University in Syracuse, N.Y., said the United States would also support India's full membership in four groups that control exports including the Nuclear Suppliers Group.

Obama announced on a visit to India in November that he was easing the restrictions, but he did not provide details at the time.

The United States and its allies slapped sanctions on India in 1998 after New Delhi shocked the world with nuclear tests. India's historic rival Pakistan carried out its own tests days afterward.

US Puts End to India Export Restrictions

But the United States soon reconciled with India. Former President George W. Bush and Prime Minister Manmohan Singh signed a deal in 2008 to cooperate on nuclear energy, despite India's refusal to join the Non-Proliferation Treaty.

The United States hopes that the agreement will allow its companies to cash in as India ramps up nuclear power to provide for a fast-growing economy.

The United States is also bidding to sell India weapons as it modernizes its military, particularly its aging air force.

Commerce Secretary Gary Locke, who called the easing of restrictions "a significant milestone in reinforcing the U.S.-India strategic partnership," plans to head to India in early February to promote high-tech trade.

He will be accompanied by 24 companies include The Boeing Co., Lockheed Martin Corp. and Westinghouse Electric Co., according to the Commerce Department.

China has also asked the United States to ease restrictions on high-tech imports, but the United States has been concerned about Beijing's economic policies and the theft of intellectual property.

Blake recommitted the United States to supporting a global role for India, but said: "It is clear that building a strong economic plank is necessary in building a strategic partnership for the future."

Blake said he was "encouraged" by signs that India will expand access to its retail sector.

"I hope that the government realizes that further openings, such as in agriculture and defense sectors, would benefit Indian consumers and its economy," he said.

Big-box U.S. retailers such as Walmart want India to ease rules that require them to partner with local firms, but many of the country's ubiquitous small shops fear they will

US Puts End to India Export Restrictions

be put out of business.

FCC Takes Steps to Free Up Wireless Spectrum

FCC takes steps to free up wireless spectrum

by [Marguerite Reardon](#)

The Federal Communications Commission took two important steps this week to free up more wireless spectrum for wireless broadband services.

On Wednesday the agency published a list of nine companies that have been granted permission to provide a database of unlicensed "white space" spectrum that can be used by device makers and service providers to offer a service that utilizes these free airwaves.

And also on Wednesday the FCC approved an order to allow a privately funded company called LightSquared to lease spectrum that was originally allocated for satellite services to use in building a terrestrial wireless service. LightSquared will use the spectrum to build a high-speed Internet network from satellite feeds. The service is aimed at companies, such as Apple and Best Buy that may want to offer mobile devices without partnering with major carriers.

Wireless experts say that more spectrum is needed to fuel the growing demand of rich services and content from consumers. The FCC has been talking about the [impending spectrum crisis](#) and has been pushing for more spectrum to be made available. In the National Broadband Plan [presented to Congress last year](#), the agency outlined a plan for freeing up 500MHz of spectrum over the next decade, with 300MHz being freed up within five years.

The agency expects to get the spectrum from various places, including some from TV broadcasters, which are no longer using spectrum that has been allocated to them. FCC Chairman Julius Genachowski has proposed a voluntary auction in which broadcasters could give up spectrum in exchange for sharing in the profits of the auction with the government. The FCC report indicates that spectrum could be worth more than \$120 billion at auction, which is twice what excess spectrum was worth in 2008.

The white space spectrum as well as reallocating spectrum that is set aside for other uses is another way to free additional spectrum. And each of the orders the agency issued yesterday with respect to wireless spectrum will help do that.

The "white space" spectrum is 300MHz to 400MHz of unused spectrum that has been used previously as buffers between TV channels. The FCC opened up the spectrum for unlicensed use and looked to private companies to maintain a database of spectrum users.

Companies, such as Microsoft and Dell [are already developing products to use the spectrum](#). In order to prevent interference, a database is needed so that devices can search for unused white spectrum in different markets.

Google is one of nine companies that has won the FCC's approval to build and manage these data bases. Other companies that will also be able to do this are Comsearch, Frequency Finder, KB

FCC Takes Steps to Free Up Wireless Spectrum

Enterprises and LS Telcom, Key Bridge, Neustar, Spectrum Bridge, Telcordia Technologies and WSdb. These companies will compile a database that shows frequencies are available in given areas. And then the companies will approve devices for use in those areas.

Because the white space spectrum is unlicensed, it will allow new players to more easily enter the wireless market. So rather than large cell phone companies or even cable companies, which have spent millions of dollars on wireless spectrum licenses, smaller companies could build a service around the unlicensed spectrum.

Google's involvement with the database is important because the company has been pushing to free up this spectrum for years. Some critics have been skeptical about Google's involvement. They warned that Google might unfairly use information made available to the database administrators, But the FCC didn't seem to feel these concerns were enough to keep Google from administering a database.

Google's Android software will likely be used in several devices that take advantage of the white space spectrum.

The databases won't be active for several weeks. Companies that have been approved as administrators have until February 28 to submit additional information about their databases. And on March 10 the FCC will hold a workshop to review the agency's rules. There will then be a 45-day trial period for each database administrator. If the companies pass the trial, they'll be able to operate their database for five years.

The FCC has asked all administrators to submit additional information about their database plans by Feb. 28 and attend a March 10 workshop to go over the agency's rules. Administrators will then undergo a 45-day trial period. If they pass the trial, they will be able to operate their databases for five-year terms.

Intel's Sandy Bridge Chipset Flaw: The Fallout

Intel's Sandy Bridge chipset flaw: The fallout
by Brooke Crothers

The [flaw Intel disclosed today](#) in its Sandy Bridge chipset was caught early in the rollout of the company's new processor, so there aren't large numbers of systems in customers' hands. But the buyer beware caveat applies, as always, to consumers.

Officially launched at this year's [CES](#), Intel's Sandy Bridge chip lineup--what Intel refers to officially as "Second Generation Intel Core Processor"--is the chipmaker's first mainstream processor to integrate graphics silicon directly onto the main processor. It is also the first chip line based fully on Intel's leading-edge 32-nanometer manufacturing process. These two features allow Intel to offer a power-efficient processor with improved multimedia and gaming capabilities.

It bears repeating that this is a chipset issue, not a Sandy Bridge processor problem. The chipset--or companion chip to the Sandy Bridge processor--is codenamed "Cougar Point." That's where the flaw resides. Chipsets, generally speaking, are conduits that allow the main processor to communicate with hardware in a PC.

And the flaw, in this case, is related to how the Cougar Point chipset communicates with [SATA devices](#), such as a SATA hard disk drive or SATA optical drive.

Bottom line: if you are a consumer who's run out and grabbed a high-end laptop or desktop gaming rig in the last few weeks with an Intel quad-core processor billed as Intel's Second Generation Intel Core Processor, then [you potentially have a problem](#).

Intel: main points of Sandy Bridge chipset flaw:

Chipset: The issue is in Sandy Bridge's Cougar Point chipset, not the main Sandy Bridge processor. Most Sandy Bridge systems sold to date are quad-core laptops, though some desktop PCs have been shipping too. Potentially affected systems have been shipping only since January 9.

Issue: Affects SATA ports 2 through 5, not ports 0 and 1. Most laptops have two SATA devices, such as a hard disk drive and optical drive that would be using the unaffected ports 0 and 1. That said, Sandy Bridge-based systems with more than a couple of SATA devices could potentially be affected. The data itself is not affected. So, if a consumer had an affected system, data could be accessed by moving the storage device to another system or a working port.

How issue was discovered: Last week customers started telling Intel that there was an issue. As Intel stressed the part, Intel's labs started seeing a failure to access ports 2 through 5. The Intel stress test simulated time passing and it showed that over time this issue could come up.

How many Sandy Bridge chipsets shipped to date: 8 million. But Intel claims relatively few are in customers' hands. Most of those are in the sales channel and will be pulled out of the channel. Intel is supporting PC makers in this effort.

Intel's Sandy Bridge Chipset Flaw: The Fallout

Issue fixed in new silicon: Intel has corrected the design issue--characterized by Intel as a "circuit design oversight"--and has begun manufacturing a new version of the chipset which will resolve the issue.

Delay of new Sandy Bridge chips: Intel expects to begin delivering the updated version of the chipset to customers in late February and expects full volume recovery in April.

Analyst's take: Nathan Brookwood of Insight 64, a chip consulting firm.

Affects consumer not corporate (enterprise): It was caught during the testing of consumer-oriented products, so when Intel finally launches Sandy Bridge processors that are targeted at enterprise--typically with vPro capability--those systems won't have the issue.

If a consumer has an early Sandy Bridge laptop: If a customer has a system with the potentially-flawed chipset, then the only real alternative is to replace the entire motherboard where the chipset has been soldered down.

Most laptops shipping today still use the previous generation of Intel processors: Because the Sandy Bridge products that use the Cougar Point chipset are just ramping now, the high-volume products continue to be last year's Core i series processors (codenamed "Westmere"). These products are not affected.

And how does this affect Intel financially? For the first quarter of 2011, Intel expects this issue to reduce revenue by approximately \$300 million as the company discontinues production of the current version of the chipset and begins manufacturing the new version. "Full-year revenue is not expected to be materially affected by the issue," Intel said. Total cost to repair and replace affected materials and systems in the market is estimated to be \$700 million.

Intel now expects first-quarter revenue to be \$11.7 billion, plus or minus \$400 million, compared to the previous expectation of \$11.5 billion, plus or minus \$400 million. Gross margin, a critical profit indicator, is now expected to be 61 percent, plus or minus a couple percentage points, compared to the previous expectation of 64 percent, plus or minus a couple percentage points.

"Obviously, no one wants to make a mistake of this magnitude. When all is said and done, we're looking at close to a billion dollars [to cover everything related to the fix]," said Dean McCarron, principal analyst at Mercury Research, a chip market research firm. "But this happened very early in the product ramp. The net impact is probably a few weeks delay in the ramp [of Sandy Bridge]," he said.

McCarron continued. "The best example, by contrast, that I can provide is Nvidia. The [\[chip\] packing problem they had](#), where you had millions of systems deployed. They took multiple hundred million dollar charges. So, a mistake like this can get very expensive if it isn't caught early," he said.

Despite the company's financial impact, McCarron said the impact on consumers is small. "We're probably talking about systems [in consumers' hands] measured in the thousands," he said.

Intel's Sandy Bridge Chipset Flaw: The Fallout

Battling a Wireless Deluge

Battling a Wireless Deluge

AT&T, Other Carriers Use Wi-Fi 'Hotzones' to Siphon Off Smartphone Traffic

By **CARI TUNA**

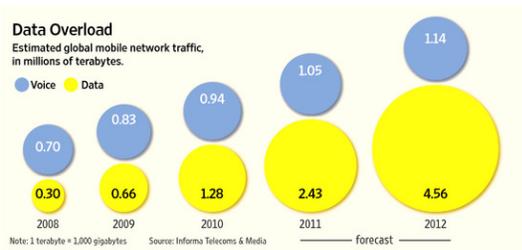
As cellular networks grapple with a deluge of data traffic from smartphones, a growing number of companies are offering to help wireless carriers shift the heavy load to a longtime Internet standby: Wi-Fi.

Suppliers of technology to help offload mobile data include behemoths such as [Cisco Systems Inc.](#) and [Motorola Solutions Inc.](#) as well as smaller vendors such as [Ruckus Wireless Inc.](#) and [BelAir Networks Inc.](#), each of which manufactures devices that transmit and receive Wi-Fi signals.

[AT&T Inc.](#), which has struggled to overcome complaints about network congestion since it started supporting [Apple Inc.](#)'s iPhone in 2007, in May launched a so-called Wi-Fi hotzone—an industry term for a large, outdoor Wi-Fi hotspot—in New York City's Times Square, in order to test the technology as a supplement to its cellular coverage.

In subsequent months, AT&T, which uses gear from BelAir and others, added hotzones in downtown Charlotte, N.C., and the neighborhood surrounding Chicago's Wrigley Field. In December, the carrier said it would add more Wi-Fi networks in New York City—including a hotzone launched last week in Rockefeller Center—as well as in San Francisco's Embarcadero Center.

Data Overload



Today, the carrier has six such Wi-Fi access zones across the U.S. and plans

Battling a Wireless Deluge

a "rapid acceleration" in its building of such networks over the coming year, said Angie Wiskocil, AT&T's senior vice president of Wi-Fi services. She called it a "cost-effective complement" to the company's 3G cellular network.

Likewise, [Towerstream Corp.](#), a Middletown, R.I., provider of high-speed Internet access to businesses, in January said it would expand a similar hotzone pilot program in New York City and add more Wi-Fi networks in cities such as Chicago and San Francisco, using gear from Ruckus Wireless. Towerstream plans to rent the networks to wireless carriers who need to reduce congestion on their 3G and 4G cellular networks.

Outside the U.S., telecommunications concerns [PCCW Ltd.](#) in Hong Kong and [China Telecom Corp.](#) have also embraced the trend. On Monday, Ruckus Wireless said a unit of China Telecom had installed more than 4,000 Wi-Fi access points across Chongqing, a major city in southwestern China, in order to augment its cellular network.

Wireless carriers are tapping Wi-Fi because it is well-suited to handle heavy data traffic at high speeds and for relatively short distances, said Gartner analyst Paul DeBeasi. Cellular technology, by contrast, "was designed to do long distances, primarily for voice, and for relatively low data speeds," he said.

Outdoor Wi-Fi access points are also smaller, easier to install and, at roughly a thousand dollars each, less expensive than cellular towers, Mr. DeBeasi said. He added, however, that Wi-Fi access points are designed to transmit signals several hundred feet, compared with a cell site's reach of several miles.

Still, Wi-Fi isn't without its drawbacks. While virtually all new smartphones have it, not all older models do, and users who do have to remember to turn on the Wi-Fi—which can drain batteries more quickly than cellular connections alone. The steps users must take to connect to hotzones vary.

Battling a Wireless Deluge

AT&T said some devices connect to its Wi-Fi networks automatically. On other devices, AT&T users must manually connect to a Wi-Fi network the first time.

In addition, Wi-Fi technology operates on unlicensed frequencies, which means that anyone can use them without government approval—a situation that can create problems if signals from multiple networks interfere with one another.

Some vendors of Wi-Fi access points are marketing technology to address that problem. But such advances haven't won over all carriers. Executives at [Sprint Nextel Corp.](#) and T-Mobile USA, a subsidiary of [Deutsche Telekom AG](#), said their companies have tested Wi-Fi systems for augmenting their cellular networks but haven't decided to deploy them.

One factor holding T-Mobile USA back is the cost of leasing space for Wi-Fi access points, which are often placed on top of buildings. "There's a point at which it's more expensive than building a cell site," said Mark McDiarmid, T-Mobile's vice president of engineering.

But at a certain density of usage "these Wi-Fi hotzones start to make a lot of sense," he added. "We're going to continue to watch the economics of this."

Verizon Wireless, which will begin selling the iPhone to U.S. customers this month, has no plans to set up Wi-Fi hotzones. There are features on cellular networks "that you don't have on Wi-Fi—the mobility, security and reliability that our customers have come to expect," said Nicola Palmer, network vice president at the carrier, which is a joint venture of [Verizon Communications Inc.](#) and [Vodafone Group PLC](#).

US Seeks Veto Powers Over New Domain Names

U.S. seeks veto powers over new domain names

by Declan McCullagh

The Obama administration is quietly seeking the power for it and other governments to veto future top-level domain names, a move that raises questions about free expression, national sovereignty, and the role of states in shaping the future of the Internet.

At stake is who will have authority over the next wave of suffixes to supplement the venerable .com, .org, and .net. At least 115 proposals are expected this year, including .car, .health, .nyc, .movie, and .web, and the application process could be finalized at a meeting in San Francisco next month.

Some are likely to prove contentious among more conservative nations. Two different groups--the [dotGAY Initiative](#) and the [.GAY Alliance](#)--already have announced they will apply for the right to operate the .gay domain; additional controversial proposals may surface in the next few months. And nobody has forgotten the [furor over .xxx](#), which has been in limbo for seven years after receiving an [emphatic thumbs-down](#) from the Bush administration.

When asked whether it supports or opposes the creation of .gay and .xxx, an official at the U.S. Commerce Department replied that "it is premature for us to comment on those domain names." The Internet Corporation for Assigned Names and Numbers ([ICANN](#)), a nonprofit based in Marina del Rey, Calif., that has a [contract](#) with the U.S. government to manage Internet addresses, is overseeing the process of adding new domain suffixes.

A statement sent to CNET over the weekend from the Commerce Department's National Telecommunications and Information Administration, or NTIA, said its proposed veto procedure "has merit as it diminishes the potential for blocking of top level domain strings considered objectionable by governments. This type of blocking harms the architecture of the DNS and undermines the goal of universal resolvability (i.e., a single global Internet that facilitates the free flow of goods and services and freedom of expression)."

Another way of phrasing this argument, perhaps, is: If less liberal governments adopt technical measures to prevent their citizens from connecting to .gay and .xxx Web sites, and dozens of nations surely will, that will lead to a more fragmented Internet.

In addition, giving governments more influence inside ICANN may reduce the odds of an international revolt that would vest more Internet authority with the [not-exactly-business-friendly United Nations](#). Last year, China and its allies [objected](#) to the fact that "unilateral control of critical Internet resources" had been given to ICANN and suggested that the U.N. would be a better fit.

Submitting an application to create and operate a new domain suffix is [expected](#) to cost \$185,000, ICANN says.

The Obama administration is proposing ([PDF](#)) that domain approval procedures be changed to include a mandatory "review" by an ICANN advisory panel comprised of representatives of

US Seeks Veto Powers Over New Domain Names

roughly 100 nations. The process is open-ended, saying that any government "may raise an objection to a proposed (suffix) for any reason." Unless at least one other nation disagrees, the proposed new domain name "shall" be rejected.

This would create an explicit governmental veto over new top-level domains. Under the procedures previously used in the creation of .biz, .name, and .info, among others, governments could offer advice, but the members of the ICANN board had the final decision.

"It's the U.S. government that's proposing this procedure, and they've shown absolutely no interest in standing up for free expression rights through this entire process," says [Milton Mueller](#), a professor of information studies at Syracuse University and author of a [recently-published book](#) on Internet governance. Mueller, who said he expects some Middle Eastern countries to object to .gay, says the Obama administration is "completely disregarding" earlier compromises.

According to the [latest version](#) of ICANN's proposed procedure, anyone may file objections to a proposed domain suffix on grounds that it may violate "norms of morality and public order," although there's no guarantee that a suffix would be rejected as a result. Two ICANN spokesmen did not respond to multiple requests for comment.

"NTIA will continue to provide advice on how ICANN can promote competition in the domain name marketplace while ensuring Internet security and stability," NTIA said in a statement. "NTIA continues to support a multi-stakeholder approach to the coordination of the domain name system to ensure the long-term viability of the Internet as a force for innovation and economic growth."

The U.S. proposal will be incorporated into what's being called a "scorecard" that governments are drafting to summarize their concerns with the current process of approving new domain suffixes. The scorecard is expected to be published in two weeks.

Then, at the end of this month, ICANN will hold a two-day meeting in Brussels with representatives of national governments to try to reach a compromise on how to share authority over new domain suffixes. (The language of the official announcement says the purpose is to "arrive at an agreed upon resolution of those differences.") ICANN's next public meeting begins March 13 in San Francisco.

A seven-page statement ([PDF](#)) in December 2010 from the national governments participating in the ICANN process says they are "very concerned" that "public policy issues raised remain unresolved." In addition to concern over the review of "sensitive" top-level domains, the statement says, there are also issues about "use and protection of geographical names." (For instance, should a U.S.-based entrepreneur be able to register .london or .paris, or should those be under governmental control?)

That statement followed years of escalating tensions between ICANN and representatives of national governments, including a [2007 statement](#) stressing the importance of "national sovereignty." A letter ([PDF](#)) sent to ICANN in August 2010 suggested that "the absence of any

US Seeks Veto Powers Over New Domain Names

controversial (suffixes) in the current universe of top-level domains to date contributes directly to the security and stability of the domain name and addressing system." And the German government recently told ([PDF](#)) ICANN CEO Rod Beckstrom that there are "outstanding issues"--involving protecting trademark holders--that must be resolved before introducing "new top-level domains."

[Steve DelBianco](#), the executive director of the [NetChoice coalition](#), says that the Obama administration's proposed veto "is not surprising." Governmental representatives "were not happy about .xxx getting through," he says. "They want a better mechanism in the future." NetChoice's members include AOL, eBay, Oracle, VeriSign, and Yahoo.

"They're looking at the rear view mirror at .xxx and looking through the windshield at several hundred new" top-level domain names, DelBianco says. "They want a mechanism that if (they) have concerns, they could stop an objectionable domain."

Using IT to Drive Innovation

Using IT to Drive Innovation

MIT professor Erik Brynjolfsson discusses how companies can increase their productivity by making better use of their data.

By David Talbot

Despite the vast amounts of computing and communication power in corporate hands, companies are at the early stages of using IT to revamp business practices, become more efficient, and drive the next wave of national productivity growth.

That's the argument made by Erik Brynjolfsson, director of the MIT Center for Digital Business at the Sloan School of Management. He says most companies still aren't using IT effectively to do things like measure the success of promotions or the performance of supply chains—data that can inspire changes that fatten revenues and ultimately benefit consumers.

He spoke with David Talbot, *Technology Review's* chief correspondent, about how leading companies use IT to test new ideas, adopt successful changes, and disseminate innovations quickly and cheaply.

TR: You've been making the case that businesses need to increase their "information metabolism." What do you mean by that?

Brynjolfsson: There have been huge advances in the underlying technology of computers and communications. But to make them effective, companies have to change their business processes and the way they organize decision making. There are many high-tech companies that are effective in using IT. Amazon and Cisco come to mind as companies that have fundamentally changed their culture, are data-driven, and use the data to drive decisions. There are also companies you don't think of as high-tech—like Harrah's [now known as Caesars Entertainment], CVS and Walmart—that have been aggressive. That doesn't necessarily mean they spend more on IT. But it does mean they use IT to rethink business processes.

In what kinds of ways? What are some examples?

Amazon runs 200 experiments a day, such as trying out different algorithms for recommending products, or changing where they put the shopping cart on the screen. When they moved the shopping cart from the left to the right of the screen, there was a few tenths of a percent improvement in the rate of abandoned shopping carts. That might not seem like much, but it's meaningful with hundreds of millions of site visits,

Using IT to Drive Innovation

and the cost of running the experiment was trivial.

That sounds like something that would come naturally for a big e-commerce company. But what about "traditional" companies?

Offline companies like Harrah's are trying different promotions and incentive systems. Harrah's has gone from being a third-tier gaming and casino company to the largest one in the world, in large part because of their use of data and analytics. They collect detailed data on customer visits with their Total Rewards card. And the culture is one of "Let's put forward a hypothesis and test it." What if you give a steak dinner or a straight discount? Maybe different demographics respond to different incentives. Then these different groups get slightly different offers. This requires a management that steps back from the traditional ego of "I know all the answers."

What other methods are companies using?

Some are using IT to replicate innovations as they are developed. They take an idea that works well in one location, embed it in software, and replicate it in thousands of locations.

So is this sort of experimentation—and rapid implementation and diffusion of improved processes—widely done?

Right now relatively few companies in the U.S. economy are using this methodology. But when [Caesars CEO] **Gary Loveman** spoke to my class at MIT, he said that what he did at Harrah's, he could have done at most of the companies in most other industries. You can see that as more companies do this, they will find better ways to increase customer satisfaction, increase efficiencies, and make supply chains work better. The scientific method brought amazing progress to the sciences. Now it's being used in management, and I expect similar results.

How do improved revenues for companies like Caesars or Walmart help consumers?

In the short run, companies that use IT see higher profits and stock market appreciation. Over time, as competitors learn how to do that, profits get competed away, and most of the benefits accrue to consumers. Ultimately, productivity growth determines living standards and the wealth of nations.

Using IT to Drive Innovation

How close are we to seeing these broader benefits?

It's fair to say that in most industries 70, 80, 90 percent of the companies aren't even close to using IT to the potential it could be used. You might have thought that companies were converging as more of them learned best practices. But we looked at the data and found that rather than firms becoming more similar, the leaders were pulling away from the laggards. That suggests to me that rather than this being a mature, stable technology, if anything, there is a new frontier opening up.

What sectors are slow to catch on?

Health care, education, and parts of manufacturing have not been as quick to embrace IT. Health care can learn lessons from other industries. I would put them 20 years behind the rest of American industry. If they can adopt some of the practices we've seen in the rest of the economy, we will see dramatically lower health costs.

How should a business get started adopting these ideas?

In my book [*Wired for Innovation: How IT Is Reshaping the Economy*] I describe seven principles of digital organization. It starts with the digitization of analog business processes, but also includes a shift toward decentralized power; broader information sharing; tighter linkage of performance to compensation; more emphasis on high-quality people and screening people who are hired; and more investment in training and education for the workforce once hired.

Right now the scarce resource is not data. We've got tons of data sitting around. According to [Google CEO] Eric Schmidt, there was more data created in the last two days than in all of history until 2000. The scarce resource is figuring out how to use the data efficiently—not with more computers, but in changing how companies are run.

Copyright Technology Review 2011.

Exabytes: Documenting the 'Digital Age' and Huge Growth in Computing Capacity

Exabytes: Documenting the 'digital age' and huge growth in computing capacity

By [Brian Vastag](#)

Washington Post Staff Writer

Thursday, February 10, 2011; 11:17 PM

Megabytes are dead.

Gigabytes are passe.

So much digital data now moves around the globe that those who endeavor to measure it employ a new - or new to non-nerds - term.

Meet the exabyte.

How much data is an exabyte? It's a billion gigabytes - and it signifies just how digital and data-intensive the world has become.

In 2007, the global capacity to store digital information - on computer hard disks, smartphones, CDs and other digital media - totaled 276 exabytes, a new report finds.

How much is that? Imagine a stack of CDs - each holding an album's worth of digital music - shooting from the top of your desk to 50,000 miles beyond the moon.

But not everyone has equal access to those resources. In fact, the digital gap between rich and poor countries appears to be growing, said Martin Hilbert of the University of Southern California, who led the audacious effort to tally all of civilization's information and computing power.

In 2002, people in developed countries had access to eight times the bandwidth - or information-carrying capacity - of people in poorer nations, Hilbert said, citing data he will publish soon. By 2007, that gap had almost doubled.

"If we want to understand the vast social changes underway in the world, we have to understand how much information people are handling," Hilbert said.

To address that question, Hilbert and co-author Priscila Lopez spent four years poring over 1,110 sources of information spanning from 1986 to 2007, including sales data from computer and cellphone makers and the music and movie industries.

In 1986, a year after digital CDs widely debuted, vinyl records still accounted for 14 percent of all

Exabytes: Documenting the 'Digital Age' and Huge Growth in Computing Capacity

data on Earth, with audiocassettes holding an additional 12 percent.

After that, the prevalence of digital media began to skyrocket. In 2002, digital storage capacity outstripped the non-digital variety - mostly paper and videotapes - for the first time.

"That was the turning point," said Hilbert, who published the report in the journal *Science*. "You could say the digital age started in 2002. It continued tremendously from there."

By 2007, the last year documented in the study, 94 percent of all information storage capacity on Earth was digital. The other 6 percent resided in books, magazines and other non-digital formats, particularly videotape, Hilbert and Lopez found.

But despite the forecasts of futurists, a paperless world has not arrived. Although stupendously outstripped in growth by digital media, the amount of paper produced for books, magazines, newspapers and office use climbed steadily over the two decades of the study.

As for computing power - the number of calculations per second available in all of the computers in the world - that grew faster than even information storage, muscling ahead at an average annual growth rate of 58 percent over 21 years. Information storage, in contrast, grew at a rate of 23 percent.

Of course, for anyone tethered to an iPhone, Gmail and Facebook all day, all of this probably comes as no surprise.

That daily digital activity contributes to a churning information tsunami. Humans generate enough data - from TV and radio broadcasts, telephone conversations and, of course, Internet traffic - to fill our 276 exabyte storage capacity every eight weeks, Hilbert said. Of course, most of the digital traffic is never stored long term, evaporating into the ether.

The study prompts deep questions, one of which Hilbert plans to explore soon: How much of this data deluge is truly useful? Or, as Hilbert distilled it, "What's the value of watching a silly cat video versus reading an overpriced book?"

While we wait for an answer, social scientists worry that the mounting data carry a hidden cost: disconnection from one another.

"We'd like to think that [information technology] changes everything, that the amazing statistics these authors cite mean that our society has fundamentally and irreversibly changed," said Thomas J. Misa, who studies the history of technology at the University of Minnesota. "I'm a bit more skeptical." After all, Misa said, "there are still secret prisons in Cairo where government agents

Exabytes: Documenting the 'Digital Age' and Huge Growth in Computing Capacity

savagely beat people. Cellphones and social media didn't change that."

Perhaps not, but widespread reports from Egypt suggest that online social networking contributed to - or even prompted - the ongoing demonstrations there.

The study also found that Earth had 3.4 billion cellphones in 2007, with telecommunications traffic growing at an average rate of 28 percent per year between 1986 and 2007. That's a lot of minutes on your plan.

In a second report Hilbert plans to publish in a few months, he found that an ever-increasing slice of our daily data resides not on home computers and the smartphones in our pockets, but in giant data warehouses owned by Google, Facebook, Citibank, the federal government and other huge entities. Microsoft's recent ad campaign touts the benefits of moving all of your personal data to "the cloud," invoking white puffs that magically - and cleanly - store our home photos.

The reality is much dirtier. In 2006, the nation's "server farms" - the home of the cloud - sucked down 1.5 percent of all electricity in the United States, double the amount used in 2000, the Environmental Protection Agency reported. Congress ordered the report out of concern that our insatiable demand for Facebook and [YouTube](#) would push the United States to build 10 new pollution-spewing coal plants.

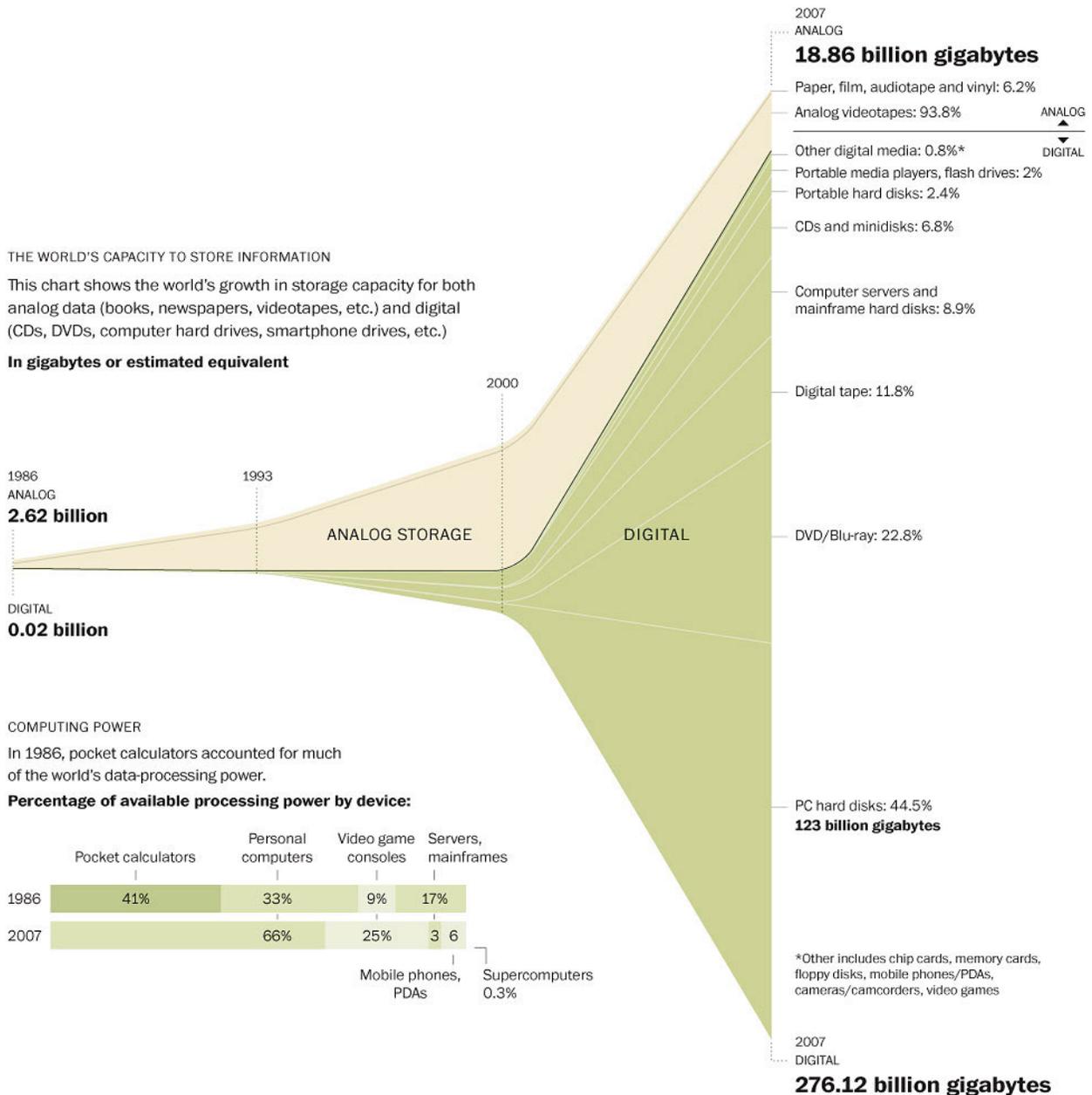
But Hilbert offers a humbling comparison. Despite our gargantuan digital growth, the DNA in a single human body still stores far more information - and a single human brain computes far more calculations - than all the technology on Earth.

"Compared to Mother Nature," Hilbert said, "we are humble apprentices."

Rise of the digital information age

In 2002, digital data storage surpassed non-digital for the first time. By 2007, 94 percent of all information on the planet was in digital form. These were among the conclusions of researchers at the University of Southern California who tried to quantify the amount of data in the world.

Exabytes: Documenting the 'Digital Age' and Huge Growth in Computing Capacity



Source: Researchers at the University of Southern California took four years -- 1986, 1993, 2000 and 2007 -- and extrapolated numbers from roughly 1,100 sources of information.

Credit: Todd Lindeman and Brian Vastag/ The Washington Post

Behind the Information Overload Hype

Behind the Information Overload Hype

By CARL BIALIK

The latest information about information overload is a lot to handle.

Wielding numbers that stretched to 20 or more digits, researchers recently reported on the world's massive ability to store, communicate and compute information. All three have grown at annual rates of at least 23% since 1986, according to a study published this month in Science.

The Numbers Guy Blog

[The World's Information Explosion](#)

Translated to a human scale, the massive numbers mean that the average person in 2007 was transmitting the informational equivalent of six newspapers per day, and receiving, in turn, 174 newspapers of data.

For data engineers, this might seem like cause for celebrating humanity's expanding universe of information. For the rest of us, it is another reminder that information is piling up at overwhelming rates.

But the digital avalanche isn't as massive as those numbers suggest. Much of the growth reflects the surge in high-resolution video and photos. In addition, while there is much more information available, each piece is being consumed, on average, by far fewer people than in the past.

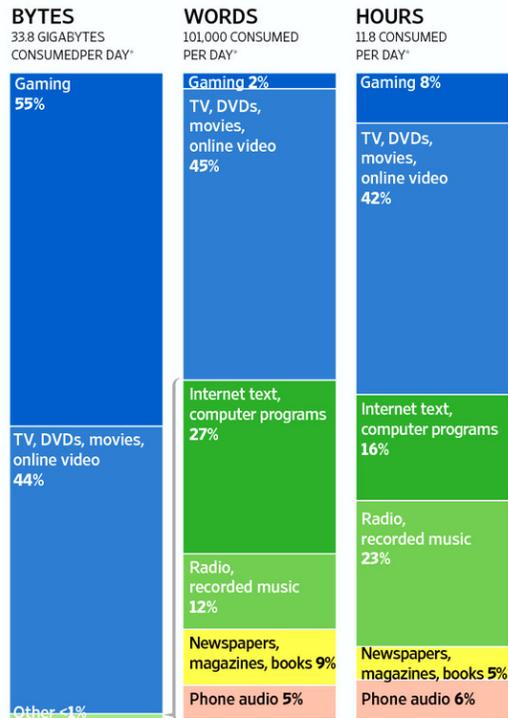
Also, heavy Internet users—think downloaders of music and movies, or digital-photo fiends—are skewing the numbers. The average person doesn't have a high-speed line, let alone the ability to read six newspapers per day.

Behind the Information Overload Hype

Parsing the Deluge

Most data reaches consumers in games or video, but those media occupy a smaller share of the information universe when gauged by words or hours instead of computer bytes.

Percentage of information consumed in the U.S. in 2008, by bytes of data and by words



*Per average American
Source: University of California, San Diego, Global Information Industry Center

Not all forms of information grew at the same pace, the Science study reveals. The amount of data stored in books roughly doubled between 1986 and 2007, a period during which the world population increased by about a third. The increase in newsprint was a relatively manageable 91%, while available storage—a barometer researchers used to estimate the quantity of information—in audio cassettes, vinyl records and photo negatives all declined. And nearly half the overall growth came from rapid improvements in hard-drive technology, making it possible to store high-resolution videos, photos and videogames as well as digital music.

Studies looking at the information glut do generally agree that there has been an enormous upsurge in information.

Behind the Information Overload Hype

The Science study—which involved compiling disparate studies of the number of various devices and their capacity—found that in 2007, humanity was able to store 295 exabytes of information. That's 295 billion gigabytes, or about 500 million times the capacity of a typical desktop computer.

One byte is equivalent to eight bits, which are the smallest units of information. A single bit is the equivalent of answering one yes-or-no question.

Martin Hilbert, the lead author of the study, says that quantifying information is vital in order to understand it.

"If you cannot express it in numbers, you cannot do science with it," says Dr. Hilbert, an economist and researcher at the University of Southern California's Annenberg School for Communication & Journalism.

Reducing all pieces of knowledge—whether pixels, words or musical notes—to digital bits makes them easier to analyze. But bits are neutral about the value of knowledge. "You can get a lot of information out of reading a half-megabyte book, compared to watching a one-gigabyte TV show," says Roger Bohn, director of the Global Information Industry Center at University of California, San Diego. Yet in 2007, the world's capacity to store video was about 6,000 times greater, in terms of bytes, than the storage capacity of paper, according to the Science study. That, says Prof. Bohn, is a "testament to how efficient language is for communicating concisely."

What is less ambiguous is that each piece of information, on average, gets less exposure today than in the past. W. Russell Neuman, professor of media technology at the University of Michigan, is leading a study that quantifies information in terms of minutes—how much time Americans devote to consuming information, and how much time it would take to consume all the available information.

In preliminary results, published online in 2009, the researchers found that in

Behind the Information Overload Hype

2005 people spent about one minute consuming media for every 1,000 minutes available—a ratio that has grown roughly tenfold since 1960.

While the amount of information is growing very fast, so might our capacity to use or filter it, says Prof. Neuman. He notes that many new tools increase ease of consumption, such as search engines and digital video recorders.

Counting the world's bytes, he says, makes the mistake of "focusing simply on capacities of machines, and not on how people are responding to the capacities of machines."

Cloud Robotics: Connect to the Cloud, Robots Get Smarter

Cloud Robotics: Connected to the Cloud, Robots Get Smarter

POSTED BY: ERICO GUIZZO / MON, JANUARY 24, 2011



Image: Cellbots

In the first “Matrix” movie, there’s a scene where Neo points to a helicopter on a rooftop and asks Trinity, “Can you fly that thing?” Her answer: “Not yet.” Then she gets a “pilot program” uploaded to her brain and they fly away.

For us humans, with our non-upgradeable, offline meat brains, the possibility of acquiring new skills by connecting our heads to a computer network is still science fiction. Not so for robots.

Several research groups are exploring the idea of robots that rely on cloud-computing

Cloud Robotics: Connect to the Cloud, Robots Get Smarter

infrastructure to access vast amounts of processing power and data. This approach, which some are calling "cloud robotics," would allow robots to offload compute-intensive tasks like image processing and voice recognition and even download new skills instantly, Matrix-style.

Imagine a robot that finds an object that it's never seen or used before—say, a plastic cup. The robot could simply send an image of the cup to the cloud and receive back the object's name, a 3-D model, and instructions on how to use it, says [James Kuffner](#), a professor at Carnegie Mellon currently working at [Google](#).

Kuffner described the possibilities of cloud robotics at the [IEEE International Conference on Humanoid Robots](#), in Nashville, Tenn., this past December. Embracing the cloud could make robots "lighter, cheaper, and smarter," he said in his talk, which created much buzz among attendees.

For conventional robots, every task—moving a foot, grasping an object, recognizing a face—requires a significant amount of processing and preprogrammed information. As a result, sophisticated systems like humanoid robots need to carry powerful computers and large batteries to power them.

According to Kuffner, cloud-enabled robots could offload CPU-heavy tasks to remote servers, relying on smaller and less power-hungry onboard computers. Even more promising, the robots could turn to cloud-based services to expand their capabilities. As an example, he mentioned the Google service known as [Google Goggles](#). You snap a picture of a painting at a museum or a public landmark and Google sends you information about it. Now imagine a "Robot Goggles" application, Kuffner suggested; a robot would send images of what it is seeing to the cloud, receiving in return detailed information about the environment and objects in it.

Using the cloud, a robot could improve capabilities such as speech recognition, language translation, path planning, and 3D mapping.

The idea of connecting a robot to an external computer is not new. Back in the 1990s, [Masayuki Inaba](#) at the University of Tokyo explored the concept of a "remote brain," as he called it, physically separating sensors and motors from high-level "reasoning" software.

Now cloud robotics seeks to push that idea to the next level, exploiting the cheap computing power and ubiquitous Net connectivity available today.

Kuffner, [who until recently was working on Google's autonomous car project](#), realized that running computing tasks on the cloud was often much more effective than trying to

Cloud Robotics: Connect to the Cloud, Robots Get Smarter

do it locally. Why couldn't robots do the same?

He's now exploring a variety of cloud robotics ideas at Google, including "using small mobile devices as Net-enabled brains for robots," he told me. Last month, some of his colleagues [unveiled their Android-powered robot software](#) and a small mobile robot dubbed the [cellbot](#) [see image above]. The software allows an Android phone to control robots based on Lego Mindstorms and other platforms.

An app store for robots

But cloud robotics is not limited to smartphone robots. It could apply to any kind of robot, large or small, humanoid or not. Eventually, some of these robots could become more standardized, or de facto standards, and sharing applications would be easier. Then, Kuffner suggested, something even more interesting could emerge: an app store for robots.

The app paradigm is one of the crucial factors behind the success of Apple's iPhone and Google's Android. Applications that are easy to develop, install, and use are transforming personal computing. What could they do for robotics?

It's too early to say. But at the Nashville gathering, attendees received Kuffner's idea with enthusiasm.

"The next generation of robots needs to understand not only the environment they are in but also what objects exist and how to operate them," says [Kazuhito Yokoi](#), head of the [Humanoid Research Group](#) at Japan's National Institute of Advanced Industrial Science and Technology (AIST). "Cloud robotics could make that possible by expanding a robot's knowledge beyond its physical body."

"Coupling robotics and distributed computing could bring about big changes in robot autonomy," said Jean-Paul Laumond, director of research at France's [Laboratory of Analysis and Architecture of Systems](#), in Toulouse. He says that it's not surprising that a company like Google, which develops core cloud technologies and services, is pushing the idea of cloud robotics.

But Laumond and others note that cloud robotics is no panacea. In particular, controlling a robot's motion—which relies heavily on sensors and feedback—won't benefit much from the cloud. "Tasks that involve real time execution require onboard processing," he says.

And there are other challenges. As any Net user knows, cloud-based applications can get slow, or simply become unavailable. If a robot relies too much on the cloud, a problem could make it "brainless."

Cloud Robotics: Connect to the Cloud, Robots Get Smarter

Kuffner is optimistic that new advances will make cloud robotics a reality for many robots. He envisions a future when robots will feed data into a "knowledge database," where they'll share their interactions with the world and learn about new objects, places, and behaviors.

Maybe they'll even be able to download a helicopter pilot program?

Below are some other examples of cloud robotics projects:

- Researchers in Singapore have built a computer cluster to generate 3-D models of environments, allowing robots to perform simultaneous localization and mapping, or SLAM, much faster.
- At LAAS, Laumond and colleagues are creating object databases for robots to simplify the planning of manipulation tasks like opening a door.
- Gostai, a French robotics firm, has built a cloud robotics infrastructure called GostaiNet, which allows a robot to perform voice recognition, face detection, and other tasks remotely. The small humanoid Nao by Aldebaran Robotics will use GostaiNet to improve its interactions with children as part of research project at a hospital in Italy.

[If you know of other cloud robotics projects, let me know.]

And here's Kuffner's powerpoint presentation:

Cloud Enabled Robots

Gorgon Stare Blinks a Lot; Testers Say Don't Field 'til Fixed

Gorgon Stare Blinks A Lot; Testers Say Don't Field Til Fixed

By [Colin Clark](#) Monday, January 24th, 2011 3:27 pm

Posted in [Air](#), [Intelligence](#), [International](#), [Policy](#)

Gorgon Stare, hailed [by the Washington Post](#) as an advanced ISR tool par excellence, should not be fielded now because it works less than the half time it should and is deemed by testers to be “not operationally suitable.”

The 53rd Wing of the Air Combat Command at Eglin Air Force Base made the recommendation in an operational utility evaluation.

Gorgon Stare is built by the Sierra Nevada Corp working under the aegis of the Air Force's vaunted Big Safari (645th Aeronautical Systems Group), charged with developing promising weapon systems quickly and getting them into use. It provides imagery from five electro-optical cameras and four infrared cameras in one pod and is supposed to be able to do day and night operations. The sensors are flown on MQ-9 Reapers.

Here's how the Post quoted a senior Air Force official about the system:

“With the new tool, analysts will no longer have to guess where to point the camera, said Maj. Gen. James O. Poss, the Air Force's assistant deputy chief of staff for intelligence, surveillance and reconnaissance. ‘Gorgon Stare will be looking at a whole city, so there will be no way for the adversary to know what we're looking at, and we can see everything.’”

Here's what Winslow Wheeler, former congressional defense budget expert and now with the Center for Defense Information, said about the system. (To his credit, Wheeler got a [hold of the test memo](#). Check the memo for the official descriptions of the problems. Wheeler summarizes below.)

His summary of the problems runs thus:

“According to DOD testers, Gorgon Stare is ineffective (‘not operationally effective’) and unreliable (‘not operationally suitable’). As described below, it cannot readily find and identify targets (especially human targets), and it cannot reliably locate what it sees. (Moving targets of any size at any location present a different problem.)

Here's his litany of Gorgon Stare woes in an email he sent:

“The 53rd Wing of the Air Combat Command at Eglin Air Force Base was tasked to test Gorgon Stare in an “operational utility evaluation.” In a draft of its test report, which I understand is fundamentally unchanged in its final form, the testers -

* found 13 “Category 1” (i.e. serious) deficiencies;

Gorgon Stare Blinks a Lot; Testers Say Don't Field 'til Fixed

* stated Gorgon Stare is “not operationally effective,” and it is “not operationally suitable.” That’s a flunk in OT&E terms: it’s both ineffective and unreliable, and recommended that Gorgon Stare not be “fielded” (deployed) to Afghanistan, or anywhere else.

“The more you read, the worse it gets:

* The imagery from Gorgon Stare is frequently marginal to poor, depending on the mode of use. Specifically, when it is used for “near real time” field or ground station use, the electro-optical (EO) imagery “can find and track [objects as small as] vehicles” but not “dismounts” (people). For contemporaneous users in the field, the Infrared (IR) imagery is worse: it is “marginally sufficient to track vehicles” and “not sufficient to track dismounts. In general, IR imagery quality is poor, which yields marginal mission capability at night.”

* In fact, Gorgon Stare may be a step backwards. The multi-camera aspect of the design seems to have created problems. Some of the imagery is “subject to gaps between stitching areas [where the camera images meet], which manifests itself as a large black triangle moving throughout the image. “Contrast differences between the four IR cameras degrade the ability to track targets across the image seams.” And, “dropped [image] frames from a few seconds to several minutes-[make] it impossible to track moving targets over that period.”

* Beyond the “seams” between images, the image quality is degraded from what users in the field have come to expect: “image quality does not support mission sets commonly used by RVT [remote video terminal] users”. In plain English, the image quality is worse than that now provided by Predator and Reaper drones without GS.

* There is a serious time delay problem. Transmissions to the ground, at the rate of two frames per second, arrive 12 to 18 seconds late for the ‘subview’ ground station, and it arrives 2 seconds late to the ‘real time’ users in the field. This “limits,” if not eliminates, the ability to track and prosecute “dynamic” (i.e. moving) targets. Of course, when the target moves to the edge (“seam”) of a camera frame, this problem becomes worse.

* The better quality imagery that is obtained from the computer pod after flight takes too long to download ‘to conduct timely forensic analysis.’

* There is another serious problem regarding the accuracy of location coordinates: ‘an unpredictable [i.e. random] software error generates a faulty coordinate grid’ rendering location information ‘inaccurate and inconsistent.’ In other words, if Gorgon Stare is ever able to find and identify a target, it might generate a false location, rendering an attempt to attack it ineffective-and hitting an unintended location which may contain innocents or friendly forces. A tester unofficially remarked that means it cannot be used for sensor or weapons cueing, a primary reason for Gorgon Stare’s existence.

Gorgon Stare Blinks a Lot; Testers Say Don't Field 'til Fixed

* Limited bandwidth is the reason for the slow data receipt; a 'work around' was established, but that reduces the quality of images even more.

Despite 'full contractor logistics,' Gorgon Stare performed poorly on measures such as 'average failures per sortie; meantime between failures; and troubleshooting time following a failure.' Overall, one tester commented that it is "about 55 to 65 percent reliable."

What really makes this noteworthy is that Gorgon Stare is exactly the kind of program that Defense Secretary Robert Gates and his acquisition leaders believe can help reshape how the Pentagon buys and develops weapons.

The reactions to the test recommendations are worrying. Wheeler says that Big Safari "claimed that the tests were unfair as they probed performance areas that were beyond the specifications for the system-just as operational testers are supposed to. Big Safari even protested that Gorgon Stare 'was designed to operate in a different environment from which is currently envisioned-relatively flat earth with a greater number of vehicles.' That would clearly exclude Afghanistan. And, therefore, they argue, it should be deployed immediately to Afghanistan!"

The argument by many technology and Pentagon advocates will be that the system has been fielded rapidly and will get much better with time, as users figure out better how to use it, maintainers figure out how to work with it and the developers improve the technology. That's all true, but this and other rapidly fielded systems must get even better as the budget crunch is likely to grow worse or they risk being scrapped for poor performance. And, of course, the troops and taxpayers deserve it.

Read more: <http://www.dodbuzz.com/2011/01/24/gordon-stare-blinks-a-lot-testers-say-dont-field-til-fixed/#ixzz1C5NzZTqq>

Air Force's 'All Seeing Eye' Flops Vision Test

Air Force's 'All-Seeing Eye' Flops Vision Test [Updated]

- By [David Axe and Noah Shachtman](#)  January 24, 2011 | 3:23 pm | Categories: [Drones](#)

It's the one of the most revolutionary — and one of the most chilling — weapons to come out of America's decade of conflicts in Afghanistan and Iraq. [Gorgon Stare](#), a new "all-seeing" camera system for aerial drones, is supposed to boost U.S. surveillance by an order of magnitude, by installing a hive of nine or more cameras under the wing of an Air Force Reaper drone. Gorgon Stare-equipped Reapers are meant to watch over a "city-size" area, while also simultaneously sending video feeds to dozens of "customers" on the ground.

There's just one problem. Gorgon Stare doesn't work as promised, at least according to the Air Force squadron whose job it is to test the new system.

In a draft report dated Dec. 30 and obtained by rogue military analyst Winslow Wheeler, the 53rd Wing at Eglin Air Force Base in Florida declared Gorgon Stare "not operationally effective" and "not operationally suitable." Alleged problems include poor-quality video, glitches in the process for downloading video streams, and a small problem of the drone blinding itself with a laser.

This is bad. Real bad. The Air Force is counting on Gorgon Stare to help its [squadrons in Afghanistan](#) meet "insatiable" demand for overhead full-motion video.

Despite steadily adding drones — there are now more than 50 three-'bot "orbits" deployed in Iraq and Afghanistan — the supply is never adequate. "It's like crack, and everyone wants more," Army Brig. Gen. Kevin Mangum said of drone-supplied video.

Equipping a portion of its drone fleet with Gorgon Stare would be like adding hundreds of new drones, from the perspective of the soldier on the ground. Now, the Air Force

Air Force's 'All Seeing Eye' Flops Vision Test

might not get that boost.

A standard drone spycam takes a “soda straw” view of what’s beneath, focusing on a lone vehicle or a single home at a time. Gorgon Stare, on the other hand, uses a bundle of cameras, each one shooting at a very slow rate and at a slightly different angle. That allows the sensor to watch over a much larger area at once: about 36 square miles or so, according to some estimates.

“Gorgon Stare will be looking at a whole city,” Air Force intelligence chief Maj. Gen. James Poss recently told *The Washington Post*. “[We can see everything.](#)”

But that view might not be so clear. The 53rd Wing found 13 serious deficiencies in the system. To carry the Gorgon Stare pod plus the required processing pod, Reapers have to be stripped of other sensors and weapons and structurally reinforced. The layout of the underwing pod puts it in the way of the Reaper’s nose-mounted ranging laser, meaning Reaper remote pilots could accidentally “lase” and blind their own cameras.

Even when working correctly, the Gorgon Stare’s cameras are “marginally sufficient to track vehicles” but “not sufficient to track dismounts [people],” the testers wrote. “In general, IR [infrared] imagery quality is poor, which yields marginal mission capability at night.”

Plus, soldiers on the ground could have a hard time capturing the Gorgon Stare’s video feed. Even if they do, a glitch in the system means imagery is “subject to gaps between stitching areas [where the camera images meet], which manifests itself as a large black triangle moving throughout the image.”

Gorgon Stare “cannot reliably find and track human targets; it has additional problems for moving targets, and the random location inaccuracy makes the system virtually

Air Force's 'All Seeing Eye' Flops Vision Test

unusable for prosecuting even stationary targets,” Wheeler summed up in an e-mail.

Gorgon Stare and other “[wide-area airborne surveillance](#)” (WAAS) systems came out of an Iraq-war imperative to [track car bombs across an entire city](#). Spycams might not be able to prevent such attacks. But if a whole town could be surveilled at once, the car bombs [could be traced back](#) to their points of origin.

As the insurgency evolved, and the Afghanistan conflict heated up, the need for WAAS changed. Instead of spotting vehicles after the fact, the military wanted WAAS to find individual, dismounted attackers — in real time.

But with a resolution at least twice as bad as standard drone cameras — and a frame rate of just 2 per second, compared to 30 in standard-issue spycams — tracking individual militants might be too tough a mission for a WAAS system. “If somebody said Gorgon Stare could spot dismounts, they probably oversold it,” says a source familiar with the programs. “It was not designed to do that.”

The 53rd Wing recommended more testing and development before Gorgon Stare gets [installed on Reapers in Afghanistan](#), something that is supposed to happen “this winter.”

We’ve asked the Air Force to respond to this report. We’ll let you know what they say.

Now, to be fair, tests are designed to uncover problems, not just rubber-stamp things that already work fine. And military testers are paid to be skeptics and trained to find even the tiniest glitch in new weapons.

That can result in unfair assessments of urgently needed weapons — and sometimes leads to clashes between testers and the broader Pentagon establishment. For example, testers for years declared the Navy’s [EA-18G radar-jamming plane](#) “not

Air Force's 'All Seeing Eye' Flops Vision Test

operationally suitable,” but the Pentagon pressed ahead with — [and even expanded](#) — plans to field the jet.

Similar assessments were made of the now-iconic Predator drone back in October 2001, when the testers found it to be not “[operationally effective or suitable](#).” It wasn’t long before the robotic spy plane was making important contributions to the war in Afghanistan.

The 53rd Wing’s assessment of Gorgon Stare could be an example of over-stringent testers striving for unnecessarily lofty benchmarks. Or the Air Force testers are correct, and the Pentagon’s revolutionary all-seeing eye really is blurry and half-blind.

Update 7:11pm: “Gorgon Stare is in the first increment of a multi-increment program, and the second increment will increase the warfighter’s capabilities by range and resolution,” Air Force spokesman Lt. Col. Richard Johnson says in a statement, released moments ago.

The document leaked was a draft memo that was later revised in January.

The January memo includes three issues that we have identified and have fixes in place. The first was addressing critical Technical Order shortfalls; the second was Gorgon Stare Ground Station image and grid coordinate generation; and the third was Remote Video Terminal compatibility. We’re working all three issues and do not believe they will affect the deployment schedule.

Air Force leadership understands the importance of providing quick, timely and actionable ISR for the field. Gorgon Stare will not be fielded until the theater commander accepts it.

The Air Force takes its responsibility seriously because lives depend on the quality of

Air Force's 'All Seeing Eye' Flops Vision Test

the intelligence products that are produced.

X-47B Robot Stealth Plane Makes First Flight

X-47B robot stealth plane makes first flight

by [Tim Hornyak](#)



The unmanned X-47B takes off at Edwards Air Force Base in California. (Credit: Northrop Grumman)

Only six years after the film "[Stealth](#)," Northrop Grumman has demonstrated its much ballyhooed [X-47B](#) robot stealth plane, successfully completing a 29-minute test flight to 5,000 feet at Edwards Air Force Base in California.

Developed under a \$635 million Navy contract, the unmanned, tailless jet provides greater range and power by taking off from aircraft carriers, delivering laser-guided bombs and refueling in the air.

The test flight, which had been expected to take place over a year ago, is a first step to demonstrating the plane on a carrier. Northrop Grumman now says that will happen in 2013 instead of this year.

The plane can fly at a "high subsonic" top speed, much faster than [UAVs](#) such as the Predator and Reaper drones.

The bat-winged X-47B has a wingspan of 62.1 feet, a maximum payload of 4,500 pounds, a host of sensor systems and a range of more than 2,100 nautical miles. It can be remotely piloted or programmed in advance for mission objectives.

It can also fly at over 40,000 feet, allowing deployments for intelligence-gathering, precision attacks and ballistic missile detection. It's slated for additional tests at Naval Air Station Patuxent River before carrier trials.

Another unmanned combat air vehicle, Britain's [Taranis](#) unmanned stealth plane is also to begin test flights this year.

Here's a clip of the X-47B's maiden flight.

X-47B Robot Stealth Plane Makes First Flight

Read more: http://news.cnet.com/8301-17938_105-20030832-1.html#ixzz1DNIPED5I

Drone Will Call Aircraft Carriers Home

Drone Will Call Aircraft Carriers Home

The Navy's X-47B, Built by Northrop Grumman, Won't Need to Be Operated From Land; Tailless Plane Passes Early Test

By [NATHAN HODGE](#)

The U.S. Navy said it made a breakthrough in drone technology with the first flight of the X-47B, a bat-winged unmanned jet designed to take off and land from an aircraft carrier, one of the most complex and difficult feats in aviation.

Capt. Jaime Engdahl, the Navy's program manager, said the most difficult part of a combat mission for Navy pilots was landing an aircraft back aboard ship. "We're making that challenge with unmanned vehicles today," he said.

The experimental aircraft, made by [Northrop Grumman Corp.](#), made its debut flight Friday, taking off from and returning to Edwards Air Force Base in California. The 29-minute flight was designed to pave the way for an eventual demonstration that the fighter-sized robotic aircraft can operate from the deck of an aircraft carrier, not just from land, as current drones do.

After initial testing at Edwards, the aircraft will be sent later this year to Naval Air Station Patuxent River in Maryland for additional land-based flights to determine the aircraft's suitability for carrier landings. The service is preparing the drone for carrier trials in 2013.

Access thousands of business sources not available on the free web. [Learn More](#)

The first flight of the X-47B highlights the dramatic evolution of unmanned aircraft in recent years, a technology the U.S. is relying on for surveillance and strike missions in the Afghanistan war. Unlike the Predator drone, which is operated by a controller on the ground, the X-47B is supposed to operate more autonomously, flying on a pre-programmed flight path.

The X-47B will be less visible to radar than most drones. The tailless aircraft has what the military calls "low observable," or LO, characteristics, though it

Drone Will Call Aircraft Carriers Home

is not a full stealth aircraft. Janis Pamiljans, Northrop program manager, described the aircraft's unique shape as "LO relevant."

In 2007, Northrop won a \$636 million award from the Navy to produce two unmanned aircraft that could operate from an aircraft carrier, beating out rival [Boeing Co.](#) for the contract. Boeing has continued to fund a stealthy, fighter-sized drone called the Phantom Ray at company expense. The Navy has not put a price tag on what future production aircraft might cost.

A rival contractor, [Lockheed Martin Corp.](#), said it contributed to some aspects of the X-47B's stealthy design, including its aerodynamic edges and control surfaces. The company also contributed to the development of the jet's tailhook system.

[View Full Image](#)



Reuters

An X-47B unmanned drone completed its first flight Friday at Edwards Air Force Base in California. The Navy hopes to test it on carriers in 2013.

If the technology proves successful, it could lead to the introduction of carrier-based drones with much longer combat ranges than manned aircraft.

Longer-range drones that can refuel in midair could help U.S. carriers stay out of harm's way far from enemy shores, making them less vulnerable to attack.

Drone Will Call Aircraft Carriers Home

A 2008 report by the Center for Strategic and Budgetary Assessments, a Washington think tank that studies military technology, said that long-range pilotless aircraft had potential to transform carriers "from a power-projection system with outstanding global mobility but relatively limited tactical reach and persistence into a key component of a global surveillance-strike network."

Peter Singer, the author of "Wired for War," a book about the revolution in military robotics, said the X-47B was "potential game-changing technology for the naval air wing," but cautioned that carrier-based drones were still a long way off. "It's the first flight of a technology that could prove to be very significant in certain combat scenarios," he said. "But it's a first flight."

After Successful First Flight, Navy Plans for Next Stage of UCAS-D Development

After Successful First Flight, Navy Plans For Next Stage of UCAS-D Development
(DEFENSE DAILY 08 FEB 11) ... Carlo Munoz

After the first successful flight of the Navy's newest unmanned reconnaissance and strike aircraft this weekend, the sea service is already preparing for an intensive test and evaluation period, culminating in the plane's full integration into Navy carrier operations, according to program officials.

Members of the Navy's Unmanned Combat Air System Program Office (PMA-268), as well as defense aviation firm Northrop Grumman [NOC], oversaw the first flight of the X-47B Unmanned Combat Air System-Demonstration (UCAS-D) aircraft.

The 29-minute flight at Edwards AFB, Calif., tested the aircraft's basic aerodynamic properties, such as speed and altitude envelopes, as well as the various avionics software and subsystems on board the demonstrator, Janis Pamiljans, UCAS-D program manager for Northrop Grumman Aerospace Systems, said in a Feb. 5 briefing. Northrop Grumman is the prime contractor on the UCAS-D effort.

The aircraft's performance "surpassed what we wanted to achieve," Pamiljans said, adding that the program was on track for a live carrier landing demonstration of the plane in 2013. To that end, the preliminary feedback from the flight test was "rock solid," matching up with pre-test modeling results by program officials, Capt. Jaime Engdahl, UCAS-D program manager at PMA-268, said during the same briefing.

Flight testing had been originally scheduled months earlier, but difficult weather conditions, combined with a handful of last-minute refinements to the platform's subsystems, pushed the flight to the right, Rear Adm. Matthew Klunder, director of intelligence, surveillance and reconnaissance capabilities in the Navy's information dominance shop (N2/N6), said during an Association of Unmanned Vehicle Systems International conference in Washington last week.

The UCAS-D, as envisioned by Navy planners, will be a unmanned, carrier-based intelligence, surveillance and reconnaissance aircraft with the ability to carry out precision strike operations.

Aside from ISR and strike capabilities, the demonstrator also proved its low observability "relevance," during the test flight, Engdahl said. Noting that low observability capability was not a requirement for the UCAS demonstrator, the now-proven swept-wing design and associated "aeroshape" factors associated with the aircraft indicated the platform would be capable of maintaining a low observability capability down the road, he noted.

Exploring the unmanned vehicle's stealth potential is only one of one of many issues program officials plan to delve into between now and 2013, Engdhal said.

With first flight now complete, UCAS-D team members with the Navy and Northrop Grumman plan to begin ground-based "flight to touchdown" tests under carrier scenarios on the UCAS-D software systems beginning in spring of this year.

After that, program officials plan to move the aircraft from Edwards AFB to Naval Air Station-Patuxent River, Md., for further "carrier sustainability" tests and related support work before the proposed 2013 flight test at sea, according to Engdhal.

After Successful First Flight, Navy Plans for Next Stage of UCAS-D Development

UCAS-D officials are also planning to begin work on a second prototype of the unmanned aircraft, set to begin this summer. The UCAS-D "Air Vehicle Two" will be designed to the same specifications as the first aircraft that was tested over the weekend, but will include an aerial refueling capability, Pamiljans said.

The second prototype will be the "primary workhorse" for testing and demonstrating air-to-air refueling for the UCAS-D system. The aircraft will utilize a boom-and-drogue system and will look to carry a maximum 2,000 pounds fuel load, he added.

While the design specifics on the refueling system are still in flux, program officials are confident that the base design tested last week will provide a solid foundation for the second aircraft, Pamiljans said, adding the first UCAS-D "can track and trail [a refueling boom] very effectively."

Company officials hope to get on contract with Naval Air Systems Command for the second UCAS demonstrator sometime in 2014, he added.

US Navy Looks to Expand Unmanned Systems

U.S. Navy Looks To Expand Unmanned Systems

Feb 4, 2011

By Michael Fabey



As the U.S. Navy refines and deploys several types of unmanned undersea and surface vessels, the service is still in the hunt for more rugged sensors, better propulsion systems and open-architecture host vehicles capable of deploying smaller unmanned systems.

The service also is interested in greater endurance and more reliable ways to refuel or recover unmanned equipment, Navy brass told attendees Feb. 3 at the Association for Unmanned Vehicle Systems International's Unmanned Systems Program Review 2011 in Washington.

But most important of all, the vehicles, sensors and systems must be affordable, according to Rear Adm. David Titley, Navy oceanographer and navigator. "I just can't emphasize how important that is for these initiatives," he says.

Gone are the days, the Navy officers say, when the Pentagon would simply fund science and technology projects for years and then move those efforts into actual programs. Now, parallel development is becoming more of the norm, with an emphasis on equipment that works now.

US Navy Looks to Expand Unmanned Systems

The Navy can cite some success stories. For example, Titley highlights an unmanned undersea glider that has already performing missions lasting four to six months in places like the Arctic or Indian oceans. Among other tasks, the gliders identify and assess water columns, providing key environmental data for anti-submarine warfare, Titley says.

“This is more than just some PowerPoint,” he says. “This is not just initial capability. We have real vehicles out in real oceans doing the Navy’s work today.”

In the immediate future, the Navy plans to deploy an unmanned surface minesweeping capability under a program called Unmanned Influence Sweep that is part of a module package for the Littoral Combat Ship (LCS), according to Capt. Duane Ashton, program manager for Navy unmanned maritime systems.

What the Navy needs from industry to make the unmanned LCS minesweeping module work, Ashton says, are ruggedized sensors that can handle rough sea states, as well as improved command-and-control equipment — especially systems that will make it possible to deploy the package long range and over the horizon.

In the longer term, Ashton says, Navy officials have bandied about the concept of a host unmanned surface ship that will be able to work in the littorals and deploy its own unmanned undersea vehicles.

Ashton and other officers say the Navy is very interested in expanding its unmanned footprint, especially under the waves. “The undersea domain is an area we haven’t tapped as much as we need to,” says Rear Adm. Mathew Klunder, director of the Navy’s Intelligence, Surveillance and Reconnaissance division.

Fire Scout to Gather Intel, Hunt Pirates

Fire Scout To Gather Intel, Hunt Pirates Feb 9, 2011

By Amy Butler
Washington



The U.S. Navy's Fire Scout will deepen its operational experience considerably both on land and at sea this year as the unmanned rotorcraft begins anti-piracy missions in the Middle East and intelligence-collection for troops in Afghanistan.

The Afghanistan deployment, including three aircraft and two ground control stations, is planned for early in the third quarter of fiscal 2011 to provide intelligence, surveillance and reconnaissance (ISR) to troops. Northrop Grumman, which manufactures the MQ-8 Fire Scout, will operate and maintain the system in theater under the guidance of Navy officers, says Victor Chen, a spokesman for Naval Air Systems Command, which manages the \$2.6 billion program. A basing decision for the rotorcraft there is expected in the next couple of weeks.

The Pentagon has called many new ISR systems into service earlier than planned to support an insatiable need for intelligence in the fight against insurgents and Al Qaeda in Afghanistan. Fire Scout carries the Brite Star II electro-optical/infrared payload, which can provide much-desired full-motion videos to soldiers, says John VanBrabant, Northrop Grumman's maritime

Fire Scout to Gather Intel, Hunt Pirates

business development manager.

Meanwhile, two Fire Scouts are deployed onboard the U.S. frigate Halyburton in Southwest Asia. Also on the frigate will be a single MH-60. Rear Adm. Matthew Klunder, director of ISR for the Navy staff, says a Fire Scout was credited with a humanitarian save last week, when it spotted a wayward boat and hovered while help was en route.

Though the Fire Scout system has yet to execute its operational evaluation (opeval) phase, Navy officials opted to deploy it on the Halyburton to provide ISR and “support anti-piracy escort of merchant shipping” in that region, Chen says. This will likely involve escorting ships off the coast of Somalia, in the Gulf of Aden and western Indian Ocean, where there has been a sharp uptick in pirate attacks.

The Halyburton sailed to the region in early January.

Officials delayed the opeval, planned for last fall, because “not all testing was completed and verified during the technical evaluation process prior to the deployment,” Chen says. Complicating last year’s tight schedule was an incident involving a lost communications link that resulted in an MQ-8 cruising into restricted airspace outside of Washington (AW&ST, Sept. 6, 2010, p. 14). Officials determined a fix for the problem and Fire Scout returned to flight in late September after nearly two months without flight trials leading up to opeval.

Navy officials now plan to conduct opeval as early as October, in the first quarter of fiscal 2012.

Once opeval flights are complete, the Navy will craft a formal report to determine whether Fire Scout is suitable and effective for its mission. If so, a full-rate production decision is likely to follow.

Eleven aircraft have been delivered to the Navy, and 19 are on contract through fiscal 2011. The Navy plans to buy 168 Fire Scouts and eventually

Fire Scout to Gather Intel, Hunt Pirates

deploy them on its new Littoral Combat Ships.

Photo: US Navy

How to Hitch a Ride to Space (for your satellite)

How to hitch a ride to space (for your satellite)

by [Rafe Needleman](#)

Got a satellite you want to pitch into orbit? India's space agency will take it, but the Indian government doesn't really want to deal with you unless you've got a "primary"--a bird larger than 200 kilograms.

Instead, businesses and universities with smaller, "secondary" satellites can hitch rides on launch vehicles designed for primaries by working with launch broker [Earth2Orbit](#), which can sell you spots on Indian launch vehicles and even help you interface your small satellite into the launch vehicle for the brief trip. Earth2Orbit will also help you sort out insurance issues.

Co-CEO Amaresh Kollipara laid out the business for me. The [Indian Space Research Organization](#) (ISRO) doesn't have the manpower to hustle for business nor the staff to deal with owners of smaller satellites. Likewise, most companies don't have access to government agencies like ISRO, [NASA](#), its Russian counterpart [Roscosmos](#), or the big commercial launch providers like [Boeing](#) or [SpaceX](#), when they want to launch a smallish satellite.



Earth2Orbit sells launch space on India's Polar Satellite Launch Vehicle, the PSLV.

How small? Anything under about 200 kilograms--and as the satellites get smaller, things get simpler. If you can fit an experiment into a cube 10 centimeters on a side, you can get a [cubesat](#) slot for about \$180,000 and get it into space in about a year and a half. Once at low Earth polar orbit, where the Indian rockets currently go, your satellite will be spring-ejected away from the primary bird for its own mission. There are only about 40 cubesats in orbit so far, but Kollipara says

How to Hitch a Ride to Space (for your satellite)

universities, especially Japanese universities, are particularly interested in the format (which, he adds, was standardized by Stanford). The cubesats are likely to also be used for testing technologies that will eventually find their ways onto primaries. (About 20 percent of Earth2Orbit's bookings are cubesats; the rest are nonstandard, larger launch units, but still under the 200 kilogram primary cutoff.)

The company is also working on a universal separation module for small satellites--basically the electrical and physical connector that satellites are attached to until they're ready to fly free.

Earth2Orbit may also get into the business of re-selling space-based imaging, which remains a multibillion-dollar market (Kollipara gives me an example: a securities analyst might want to be able to count [cars](#) in Wal-Mart parking lots on given days--and you can't necessarily get that from Google).

At the moment the company only brokers spots in ISRO's low Earth orbit satellites, but Kollipara tells me he's hoping to be able to offer a similar service on Russian rockets.

Like the benign but parasitic launch slots it sells, Earth2Orbit itself is an opportunistic, small (seven-person) company riding on the large, capital-intensive, and highly risky space launch business. It's a good business, human-intensive, and hard to break in to, based on hard-to-forge relationships with government agencies. There's no cost of goods, just salaries--at least until the company gets into buying imaging data and manufacturing launch separation modules.

While information and commerce brokerages can be good businesses for a while, there is always a risk that the organizations that own the services being brokered could cut out middlemen and go direct to the customers. It is, however, unlikely that a space agency would prefer that; using a private company as the interface to private industry seems to make sense. And with deliberate, large government agencies, it would be easy to see such a change coming. If that does happen, Earth2Orbit's other services may be able to fill in the gap.

Weather Sat Program Slammed

Weather Sat Program Slammed

By [Colin Clark](#) Tuesday, February 1st, 2011 2:10 pm

The White House, Congress NASA, NOAA, Defense Department and prime contractor Northrop Grumman failed time and again in their management and oversight of the multi-billion dollar weather satellite program known as NPOESS. The failures led to huge cost overruns, long schedule delays and scarred the space acquisition community for years. Perhaps most significantly for the long haul, it left behind a sense of distrust and discord between the Department of Defense, NASA and the Commerce Department, making interagency cooperation a greater challenge than ever.

Those are the findings of a wide-ranging and authoritative study of the program by the Aerospace Corp., a federally-funded research corporation that does most of its work for the Air Force, combined with insights offered by a former senior Pentagon official who played a key role on overseeing the program for several years. The NPOESS program was designed to provide crucial weather data to the military and to civilian agencies.

“What happened was a series of unfortunate events. If only one of them had happened it could have been recoverable, but mistake after mistake was made,” said Josh Hartman, who should know, having served as one of congressional aides overseeing the program and as the Pentagon official directly responsible for overseeing space acquisition as advisor to the head of OSD acquisition.

The program received its initial and hardest push from Vice President Al Gore, who believed placing the sensors of several weather satellites on one platform would save money and provide the United States with unparalleled weather capabilities at a reasonable cost.

The Aerospace Corp. briefing on the program notes that the vice president hoped to “claim a small portion of the Peace Dividend by converging the military and civil weather satellite programs.”

That didn’t work very well, as Hartman notes: “We thought it would be a wise idea to place nine sensors on a single platform. That gave us nine long poles in the tent. When you manage a program with nine poles it’s really difficult to get the tent up.”

And Gore’s support for the program did not mean that NOAA, the Pentagon and NASA stopped believing that White House support for the program vanished when Gore lost the election. Instead, the perception of White House support became a complicating factor in efforts to amend the program, Hartman says: “The fact this was a presidential matter of interest made it more difficult to go back and fix it.”

Here are some of the other main findings of the Aerospace Corp. study:

Weather Sat Program Slammed

“Chronically unrealistic cost estimation tainted the budget process, dictated the acquisition strategy, distorted management decisions, and set the program up for cost overruns.

“The government and the prime contractor failed to establish clear, detailed supplier performance expectations and appropriate incentives.”

The acquisition strategy was built on two “major flaws”

There weren’t enough “talented, sufficiently experienced staff.” Those staff “were a root cause of program execution problems.”

The management structure — spread between NASA, NOAA, the Office of Secretary of Defense and the Air Force — made it very difficult to make sound program decisions.

If you spoke with congressional staff, senior program officials and some industry insiders during the program’s worst period several years ago, they would admit that the hydra-headed management system made it extremely difficult to find out what was happening, let alone fix the program. “It seemed like there were multiple heads trying to manage the program,” is the way Hartman generously put it.

In addition to the larger structural problems cited above, the program’s most important sensor, known as VIIRS, encountered problem after problem. It was so technically advanced that its builder, Raytheon, had great trouble making it work correctly. The government failed to award a second contract to force Raytheon to compete in building the sensor, the study finds. Also, the requirements were so demanding they were difficult to meet. And the “contract value was severely underpriced.” In the long run, VIIRS “was the major cause of schedule delays” and ate up considerable amounts of the extra money pumped into the program to bring things back into line after the program was restructured after its Nunn-McCurdy breach in 2005.

Finally, Hartman notes that the most lasting damage may have been done to the interagency acquisition and decision processes.

“It came at great cost and, more notably, it came with much emotional tension through the actions of the interagency partners. They spent much political equity because they were not working well together,” he said. “There is something to be learned from this. We can’t necessarily do interagency program management, and we’ve got to find a way to do that successfully.”

After years of expressing anguish, the White House finally broke the program apart in February and ordered NOAA, NASA and the Pentagon to come up with new plans. That led to the Defense Weather Satellite System (DWSS), which was approved Aug. 13 by Ash Carter, undersecretary of defense for acquisition, technology and logistics, and the Joint Polar Satellite System. DWSS will cost around \$5 billion. Northrop will build the new bird and it will carry VIIRS (Visible Infrared Imager Radiometer Suite), and a microwave sensor. The two satellite systems will be commanded by and send

Weather Sat Program Slammed

their data through a common ground station system managed by NOAA and by NASA. NASA will manage the JPSS — not NOAA.

Russia Loses Military Satellite

Russia loses military satellite: reports

AGENCE FRANCE-PRESSE

Published: 1 Feb 2011 15:51

MOSCOW - Russia's top military and space official launched a search Tuesday for a missing military satellite that apparently was put into the wrong orbit shortly after its launch.

The Russian defense ministry confirmed that it had lost sight of the craft - a dual-use vessel that can draw a three-dimensional map of the Earth and locate the precise positions of various targets.

The incident came just a month after President Dmitry Medvedev sacked two top space officials for a similar setback and delivered another humiliating blow to Russia's much-maligned space industry.

The seriousness of the situation was underscored late Tuesday by reports that the defense ministry had set up an urgent joint task force with the Russia's space agency to look for the missing craft.

The Geo-IK-2 satellite was created in Russia to help the military survey land and create a detailed three-dimensional map of the Earth. It was designed to spin in a circular orbit 1,000 kilometers (600 miles) above ground.

But news reports said that the satellite had been put in an elliptical orbit whose lowest point brought it to within 330 kilometers of Earth.

"We have still not been able to establish contact with the craft, and it looks like most likely, it will be declared lost," a Russian space source told the Interfax-AVN news service.

"The spacecraft will not be able to perform its intended functions at these orbit characteristics," another space official told the news agency.

Russia Loses Military Satellite

Reports pointed the initial blame for the failure on the satellite's Briz-KM upper stage rocket.

The satellite's launch had already been delayed from December because of technical malfunctions that were detected at its northern Russian launch site in Plesetsk.

Tuesday's malfunction came less than five weeks after Medvedev fired two top space officials and reprimanded the space agency chief for a launch failure caused Russia to delay the deployment of its own navigation system.

Russia's Proton-M rocket had on that occasion proven too heavy to reach its initial orbit and had been forced to dump its three high-tech Glonass-M satellites near the Hawaii Islands.

Investigators said that accident was caused by a basic fuel miscalculation that made the craft too heavy to reach its required height.

The three Glonass satellites would have completed a system whose research had been started by the Soviet Union in 1976.

China Develops Counterspace Weapons

China Develops Counterspace Weapons: DoD Deputy

By KARIN ZEITVOGEL, AGENCE FRANCE-PRESSE

Published: 4 Feb 2011 16:56

WASHINGTON - China is developing "counterspace" weapons that could shoot down satellites or jam signals, a Pentagon official said Feb. 4, as the United States unveiled a 10-year strategy for security in space.

"The investment China is putting into counterspace capabilities is a matter of concern to us," deputy secretary of defense for space policy Gregory Schulte told reporters as the defense and intelligence communities released their 10-year National Security Space Strategy (NSSS).

The NSSS marks a huge shift from past practice, charting a 10-year path in space to make the United States "more resilient" and able to defend its assets in a dramatically more crowded, competitive, challenging and sometimes hostile environment, Schulte said.

"Space is no longer the preserve of the US and the Soviet Union, at the time in which we could operate with impunity," Schulte said.

"There are more competitors, more countries that are launching satellites ... and we increasingly have to worry about countries developing counterspace capabilities that can be used against the peaceful use of space. China is at the forefront of the development of those capabilities."

U.S. concerns over China's space activities have led Defense Secretary Robert Gates to seek to include space in the stability dialogue with the Chinese, Schulte said.

In 2007, China shot down one of its own weather satellites using a medium-range ground missile, sparking international concern not only about how China was "weaponizing" space, but also about debris from the satellite.

China Develops Counterspace Weapons

Years later, Chinese space junk is still floating around in space. Last year, debris from the satellite passed so close to the International Space Station that crew members had to change orbit and take cover.

Shooting down the satellite not only focused the world's attention on the amount of junk in space but also on Chinese counterspace capabilities, which go beyond shooting down spacecraft, Schulte said.

Among other counterspace activities, Beijing has jammed satellite signals and is developing directed energy weapons, which emit energy towards a target without firing a projectile, said Schulte.

And China isn't the only country flexing its counterspace muscle. Iran and Ethiopia are, too, he said.

"They've jammed commercial satellites. ... If Ethiopia can jam a commercial satellite, you have to worry about what others can do against our military satellites," Schulte said.

"Fifteen years ago we didn't have to worry about that, but now we have to think differently, to think about how we can continue to conduct the critical functions that are performed from space, or, if they're degraded, we have to have alternative solutions."

The 10-year strategy document proposes ways to protect U.S. space assets, including by setting up international partnerships along the lines of NATO, under which an attack on one member would be an attack on all, drawing a unified response from members of the alliance.

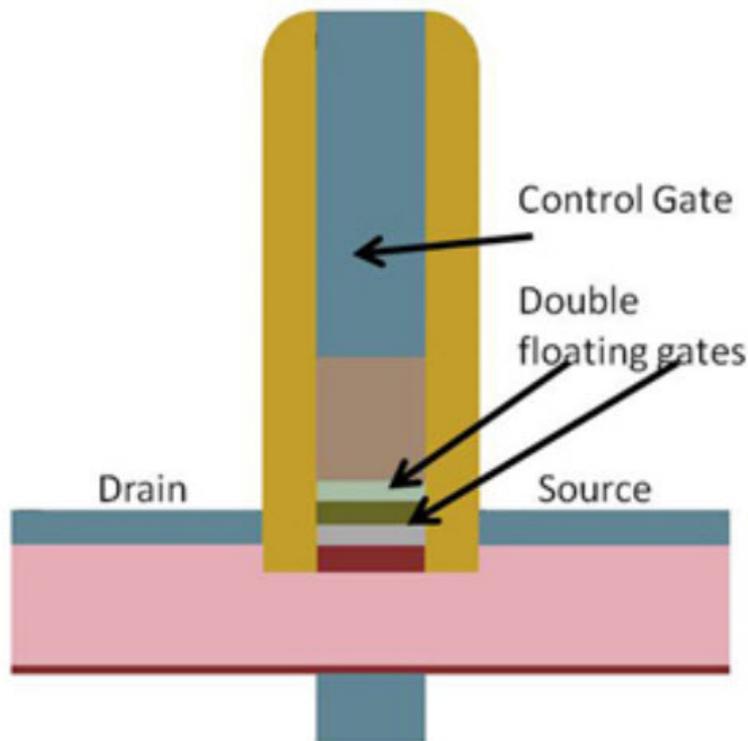
The United States also "retains the option to respond in self-defense to attacks in space, and the response may not be in space, either," Schulte said.

'Universal' Memory Aims to Replace Flash and DRAM

'Universal' memory aims to replace flash and DRAM

January 25, 2011 by Editor

[+]



Unified device can perform both volatile and nonvolatile memory operations

Researchers from North Carolina State University have developed a single “unified” device that can perform both volatile and nonvolatile memory operation, with applications that could improve computer start times and energy efficiency for Internet servers.

“We’ve invented a new device that may revolutionize computer memory,” says Dr. Paul Franzon, a professor of electrical and computer engineering at NC State and co-author of a paper describing the research. “Our device is called a double floating-gate field effect transistor (FET).”

Existing nonvolatile memory* used in data storage devices utilizes a single floating gate, which stores charge in the floating gate to signify a 1 or 0 (one bit). By using two floating gates, the device can store a bit in a nonvolatile mode, and/or it can store a bit

'Universal' Memory Aims to Replace Flash and DRAM

in a fast, volatile mode, like the normal main memory on your computer.”

The double floating-gate FET could have a significant impact on a number of computer problems. For example, it would allow computers to start immediately, because the computer wouldn't have to retrieve start-up data from its hard drive — the data could be stored in its main memory.

The new device would also allow “power proportional computing.” For example, Web server farms, such as those used by Google, consume an enormous amount of power — even when there are low levels of user activity — in part because the server farms can't turn off the power without affecting their main memory.

“The double floating-gate FET would help solve this problem,” Franzon says, “because data could be stored quickly in nonvolatile memory — and retrieved just as quickly. This would allow portions of the server memory to be turned off during periods of low use without affecting performance.”

Franzon also notes that the research team has investigated questions about this technology's reliability, and that they think the device “can have a very long lifetime, when it comes to storing data in the volatile mode.”

The paper, “Computing with Novel Floating-Gate Devices,” will be published Feb. 10 in IEEE's *Computer*. The paper was authored by Franzon; former NC State Ph.D. student Daniel Schinke; former NC State master's student Mihir Shiveshwarkar; and Dr. Neil Di Spigna, a research assistant professor at NC State. The research was funded by the National Science Foundation.

* Traditionally, there are two types of computer memory devices. Slow memory devices are used in persistent data storage technologies such as flash drives. They allow us to save information for extended periods of time, and are therefore called nonvolatile devices. Fast memory devices allow our computers to operate quickly, but aren't able to save data when the computers are turned off. The necessity for a constant source of power makes them volatile devices.

'Universal' Memory Aims to Replace Flash and DRAM

Adapted from [materials](#) provided by North Carolina State University

Micron to Reveal Tech It Says Increases Chip Speed 2-Fold

Micron to reveal tech it says increases chip speed 20-fold

by [Brooke Crothers](#)

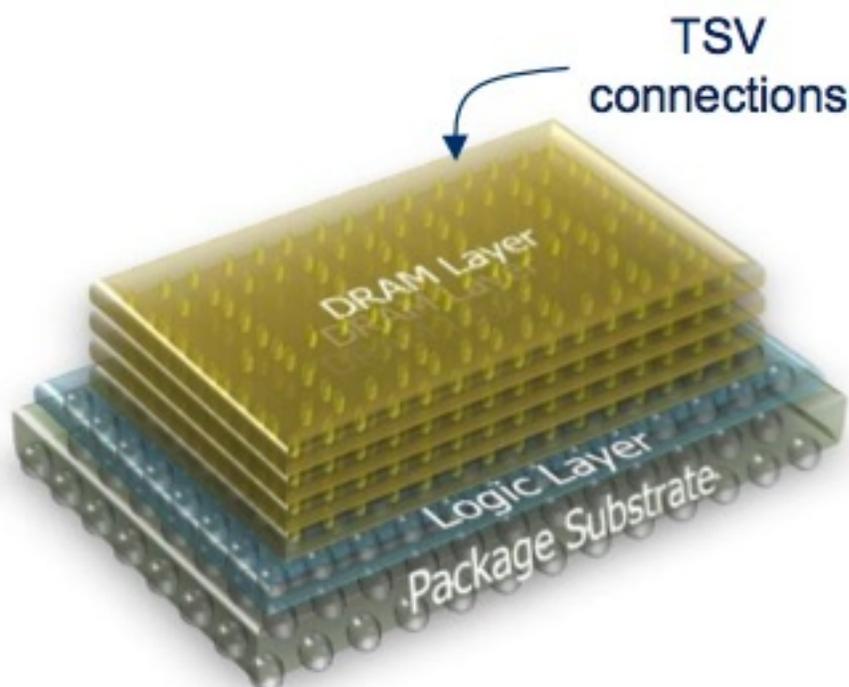
Micron Technology tomorrow is set to disclose a hybrid memory technology that it claims will boost performance 20-fold over the memory chips used in PCs today.

Micron, the largest manufacturer of memory chips in the U.S., says the "Hybrid Memory Cube" can tap into the full performance potential of DRAM--or dynamic random access memory--resolving a longstanding problem referred to as the "memory wall."

Targeted initially at networking and high-performance computers, the technology will be rolled out at an investor conference in Phoenix, Ariz.

"Where DRAM is positioned in the system, you really get into some intractable performance bottlenecks," said Brian M. Shirley, vice president of DRAM Solutions at Micron, in a phone interview on Tuesday. "As you move to new memory technologies, the computer is not able to take advantage of that extra performance. This is true for not just Micron but for everyone (all memory chip makers). It's something called the 'memory wall,'" he said.

Micron to Reveal Tech It Says Increases Chip Speed 2-Fold



Functioning prototypes in silicon **TODAY**

Micron uses through-silicon via (TSV) technology to stack memory on top of a controller chip ('logic layer'). The on-chip controller is the key to delivering the performance boost.
(Credit: Micron Technology)

Essentially, the performance of DRAM is constrained by the capacity of the data channel that sits between the memory and the processor. No matter how much faster the DRAM chip itself gets, the channel often becomes a choke point for data.

Today, DRAM technology used in PCs is most commonly referred to as DDR3, or Double Data Rate 3.

"There's a growing wall between the kind of performance we can get off the DRAM and then getting all of that data over to the processor itself. If you look at the move recently from DDR2 to DDR3 memory, it was the first transition that I can remember where the desktop and notebook guys actually delayed their transition because in terms of real, absolute performance, they weren't seeing a big enough benefit from DDR2 to DDR3," he said.

Shirley continued. "We've rearchitected in a way to get through this memory wall and deliver a staggering amount of DRAM bandwidth directly to the processor," he said. "20X. Those are real

Micron to Reveal Tech It Says Increases Chip Speed 2-Fold

numbers. A credible, defensible number. And there's room to grow on top of that."

The secret sauce is the memory controller (see graphic) that's been added to the memory. "By putting this logic layer--which is actually a controller chip--we were able to overcome that bottleneck by crafting a higher speed bus that will go from the [controller] chip to the CPU. A very, very high-speed bus," he said.

Micron is currently working with high-performance computing and networking companies but, like most high-performance technologies, this is expected to work its way to the consumer space in some form. "We would see this working its way to commercial (corporate) solutions as early as 2012, with significant volumes in 2013. These kind of technologies will start to work their way toward the consumer space in 2015, 2016," he said.

For now, the performance needs are most dire in networking and cloud computing. One-hundred gigabit Ethernet routers and switches and cloud computing servers require "everything they can get," he said. "This is our way of giving them a fire hydrant."

Micron, unlike the multitude of "fabless" semiconductor design houses in the world, is also one of the world's largest manufacturers of memory chips, with large plants in Idaho, Utah, and Virginia, among other locations. Like Intel--with which Micron has a flash-memory chip manufacturing joint venture--Micron actually builds the technologies it develops.

Customers will include major processor suppliers. Though no customers have been named yet, it would probably be safe to assume that one of those companies is Intel, the largest chipmaker in the world.

Micron will also continue to work on next-generation memory technologies for the consumer space, such as DDR4, Shirley said.

NAVAIR Working with Army to Develop New Wide-Area Surveillance Capability

NAVAIR Working With Army To Develop New Wide-Area Surveillance Capability
(DEFENSE DAILY [02 FEB 11](#)) ... Carlo Munoz

The Navy is working with its counterparts at Army aviation to create a new wide-area surveillance capability for the ground service's fleet of aerostats and unmanned aerial vehicles, according to a recent contract award issued by the Navy's air warfare center.

The \$10.4 million contract awarded to Arlington, Va.-based Logos Technologies will cover "systems integration and testing support" of the Army's Lightweight Expeditionary Airborne Persistent Surveillance-Overseas Contingency Operations (LEAPS-OCO) system and transition that work into the remainder of the service's unmanned aircraft, a Jan. 26 award notice issued by the Naval Air Warfare Center's aircraft division states.

The LEAPS-OCO system has already been fielded on board the Army's low-altitude Shadow UAS, and is being used to "detect unfriendly personnel, under day and night conditions, involved in potential attacks on the [forward operating bases], emplacement of improvised explosive devices and any other terrorist activity," the Navy notice states.

The LEAPS-OCO system is currently deployed on board the ground service's Shadow tactical UAS aircraft in Iraq, Afghanistan and other locations across the globe.

The results from that integration and testing support for the Army sensor program will feed into the center's work toward "design, development, production, fielding, operation and sustainment" of a new Wide-Area Persistent Surveillance (WASP) system.

The initiative is tied to Naval Air Warfare Command's "special surveillance programs" effort run out of NAS Partuxent River, Md. At press time, a NAVAIR spokesman had not replied to queries regarding the details of the contract, or the nature of the Army-Navy collaboration on the effort.

The two-year development time line for the WASP, covered by the Jan. 26 contract, will focus on development of enhanced data storage technologies for wide-area surveillance, as well as force protection and "false alarm mitigation" applications for U.S. forces engaged in combat operations.

The data storage aspect of the program, as planned, will "provide improved tracking of dismounted personnel in and around a forward operating base," the award notice states. To provide ground forces with a false alarm mitigation capability, company officials will look to leverage "demonstrated technologies to reduce false positives and reduce the danger to U.S. and coalition personnel," the notice states.

Aside from actual WASP sensor development, testing and operation, officials from Logos Technologies will also be responsible for configuration of the sensor to work with the Persistent Ground Surveillance System (PGSS), as well as "the design, documentation and building of interfaces that allow the...aerostat-mounted sensor and ground support segments to interface with [the] Persistent Threat Detection System (PTSD)," it adds.

Logos Technology was awarded the contract via a single-source competition, based on the company's past involvement in the program. The firm was awarded the first and second phase of the development effort when it was being conducted by the Defense Advanced Research Projects Agency, under its small business innovation initiative.

The current contract with NAVAIR represents the third phase of the WASP development.

NAVAIR Working with Army to Develop New Wide-Area Surveillance Capability

Next Generation Super Computers

Next-Generation Supercomputers

Supercomputers are now running our search engines and social networks. But the heady days of stunning performance increases are over

By PETER KOGGE / FEBRUARY 2011

Supercomputers are the crowning achievement of the digital age. Yes, it's true that yesterday's supercomputer is today's game console, as far as performance goes. But there is no doubt that during the past half-century these machines have driven some fascinating if esoteric pursuits: breaking codes, predicting the weather, modeling automobile crashes, simulating nuclear explosions, and designing new drugs—to name just a few. And in recent years, supercomputers have shaped our daily lives more directly. We now rely on them every time we do a Google search or try to find an old high school chum on Facebook, for example. And you can scarcely watch a big-budget movie without seeing supercomputer-generated special effects.

So with these machines more ingrained than ever into our institutions and even our social fabric, it's an excellent time to wonder about the future. Will the next decade see the same kind of spectacular progress as the last two did?

Alas, no.

Modern supercomputers are based on groups of tightly interconnected microprocessors. For decades, successive generations of those microprocessors have gotten ever faster as their individual transistors got smaller—the familiar Moore's Law paradigm. About five years ago, however, the top speed for most microprocessors peaked when their clocks hit about 3 gigahertz. The problem is not that the individual transistors themselves can't be pushed to run faster; they can. But doing so for the many millions of them found on a typical microprocessor would require that chip to dissipate impractical amounts of heat. Computer engineers call this the power wall. Given that obstacle, it's clear that all kinds of computers, including supercomputers, are not going to advance at nearly the rates they have in the past.

So just what can we expect? That's a question with no easy answer. Even so, in 2007 the U.S. Defense Advanced Research Projects Agency ([DARPA](#)) decided to ask an even harder one: What sort of technologies would engineers need by 2015 to build a

Next Generation Super Computers

supercomputer capable of executing a quintillion (10^{18}) mathematical operations per second? (The technical term is floating-point operations per second, or flops. A quintillion of them per second is an exaflops.)

DARPA didn't just casually pose the question. The agency asked me to form a study group to find out whether exaflops-scale computing would be feasible within this interval—half the time it took to make the last thousandfold advance, from teraflops to petaflops—and to determine in detail what the key challenges would likely be. So I assembled a panel of world-renowned experts who met about a dozen times over the following year. Many of us had worked on today's petaflops supercomputers, so we had a pretty good idea how hard it was going to be to build something with 1000 times as much computing clout.

We consulted with scores of other engineers on particular new technologies, we made dozens of presentations to our DARPA sponsors, and in the end we hammered out a [278-page report \[PDF\]](#), which had lots of surprises, even for us. The bottom line, though, was rather glum. The practical exaflops-class supercomputer DARPA was hoping for just wasn't going to be attainable by 2015. In fact, it might not be possible anytime in the foreseeable future. Think of it this way: The party isn't exactly over, but the police have arrived, and the music has been turned way down.

This was a sobering conclusion for anyone working at the leading edge of high-performance computing. But it was worrisome for many others, too, because the same issues come up whether you're aiming to construct an exaflops-class supercomputer that occupies a large building or a petaflops-class one that fits in a couple of refrigerator-size racks—something lots of engineers and scientists would dearly like to have at their disposal. Our panel's conclusion was that to put together such "exascale" computers—ones with DARPA's requested density of computational might, be they building-size supercomputers or blazingly fast rack-size units—would require engineers to rethink entirely how they construct number crunchers in the future.

How far away is an exaflops machine? A decent supercomputer of the 1980s could carry out about a billion floating-point operations per second. Today's supercomputers exceed that by a factor of a million. The reigning champion today is China's Tianhe-1A

Next Generation Super Computers

supercomputer, which late last year achieved a world-record 2.57 petaflops—that's 2.57 quadrillion (2.57×10^{15}) flops—in benchmark testing. Still, to get to exaflops, we have a factor of almost 400 to go.

The biggest obstacle to that by far is power. A modern supercomputer usually consumes between 4 and 6 megawatts—enough electricity to supply something like 5000 homes. Researchers at the University of Illinois at Urbana-Champaign's National Center for Supercomputing Applications, IBM, and the Great Lakes Consortium for Petascale Computation are now constructing a supercomputer called Blue Waters. In operation, this machine is going to consume 15 MW—more actually, if you figure in what's needed for the cooling system. And all that's for 10 petaflops—two orders of magnitude less than DARPA's exaflops goal.

If you tried to achieve an exaflops-class supercomputer by simply scaling Blue Waters up 100 times, it would take 1.5 gigawatts of power to run it, more than 0.1 percent of the total U.S. power grid. You'd need a good-size nuclear power plant next door. That would be absurd, of course, which is why DARPA asked our study group to figure out how to limit the appetite of such a computer to a measly 20 MW and its size to 500 conventional server racks.

"A modern supercomputer usually consumes between 4 and 6 megawatts—enough electricity to supply something like 5000 homes."

To judge whether that is at all feasible, consider the energy expended per flop. At the time we did the study, computation circuitry required about 70 picojoules for each operation, a picojoule being one millionth of one millionth of a joule. (A joule of energy can run a 1-watt load for one second.)

The good news is that over the next decade, engineers should be able to get the energy requirements of a flop down to about 5 to 10 pJ. The bad news is that even if we do that, it won't really help. The reason is that the energy to perform an arithmetic

Next Generation Super Computers

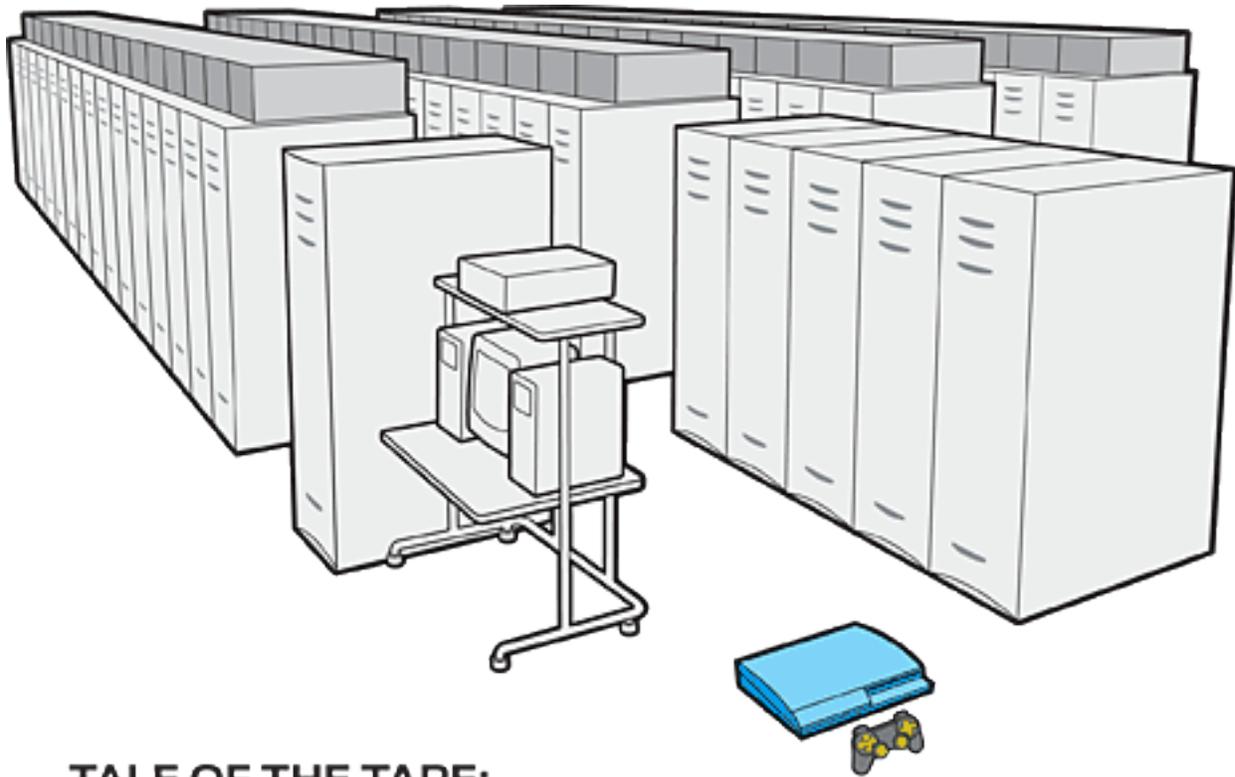
operation is trivial in comparison with the energy needed to shuffle the data around, from one chip to another, from one board to another, and even from rack to rack. A typical floating-point operation takes two 64-bit numbers as input and produces a 64-bit result. That's almost 200 bits in all that need to be moved into and out of some sort of memory, likely multiple times, for each operation. Taking all that overhead into account, the best we could reasonably hope for in an exaflops-class machine by 2015 if we used conventional architecture was somewhere between 1000 and 10 000 pJ per flop.

Once the panel members realized that, we stopped thinking about how to tweak today's computing technology for better power efficiency. We'd have to start with a completely clean slate.

To get a handle on how best to minimize power consumption, we had to work out a fairly detailed design for the fundamental building block that would go into making up our hypothetical future supercomputer. For this, we assumed that the microprocessors used would be fabricated from silicon, as they are now, but using a process that would support chip voltages lower than the 1 volt or so that predominates today. We picked 0.5 V, because it represented the best projection for what industry-standard silicon-based logic circuitry would be able to offer by 2015. Lowering the operating voltage involves a trade-off: You get much lower power consumption, because power is proportional to the square of voltage, but you also reduce the speed of the chip and make circuits more prone to transient malfunctions.

Bill Dally (then at Stanford and now chief scientist of Nvidia Corp.), working largely on his own, hammered out the outlines of such a design on paper. The basic module he came up with consists of a chip with 742 separate microprocessor cores running at 1.5 GHz. Each core includes four floating-point units and a small amount of nearby memory, called a cache, for fast data access. Pairs of such cores share a somewhat slower second-level cache, and all such pairs can access each other's second-level (and even third-level) memory caches. In a novel twist, Dally's design has 16 dynamic RAM chips directly attached to each processor. Each processor chip also has ports for connections to up to 12 separate routers for fast off-chip data transfers.

Next Generation Super Computers



TALE OF THE TAPE: SUPERCOMPUTER VS. GAME CONSOLE

	SANDIA LAB'S ASCI RED	SONY PLAYSTATION 3
DATE OF ORIGIN	1997	2006
PEAK PERFORMANCE	1.8 teraflops	1.8 teraflops*
PHYSICAL SIZE	150 square meters	0.08 square meter
POWER CONSUMPTION	800 000 watts	<200 watts

* For GPU; CPU adds another 0.2 teraflops

Illustration: George Retseck

One of these processor-memory modules by itself should be able to perform almost 5 teraflops. We figured that 12 of them could be packaged on a single board and that 32 of these boards would fit in a rack, which would then provide close to 2 petaflops,

Next Generation Super Computers

assuming the machine was running at peak performance. An exaflops-class supercomputer would require at least 583 such racks, which misses DARPA's target of 500 racks but is nevertheless a reasonable number for a world-class computing facility.

The rub is that such a system would use 67 MW, more than three times the 20 MW that DARPA had set as a limit. And that's not even the worst problem. If you do the arithmetic, you'll see that our 583-rack computer includes more than 160 million microprocessor cores. It would be tough to keep even a small fraction of those processors busy at the same time.

Realistic applications running on today's supercomputers typically use only 5 to 10 percent of the machine's peak processing power at any given moment. Most of the other processor cores are just treading water, perhaps waiting for data they need to perform their next calculation. It has proved impossible for programmers to keep a larger fraction of the processors working on calculations that are directly relevant to the application. And as the number of processor cores skyrockets, the fraction you can keep busy at any given moment can be expected to plummet. So if we use lots of processors with relatively slow clock rates to build a supercomputer that can perform 1000 times the flops of the current generation, we'll probably end up with just 10 to 100 times today's computational oomph. That is, we might meet DARPA's targets on paper, but the reality would be disappointing indeed.

The concerns we had with this approach did not end there. Accessing memory proved especially vexing. For example, in analyzing how much power our hypothetical design would use, we assumed that only 1 out of every 4 floating-point operations would be able to get data from a nearby memory cache, that only 1 out of every 12 memory fetches would come from a separate memory chip attached to the microprocessor chip, and only 1 out of every 40 of them would come from the memory mounted on another module. Real-world numbers for these things are invariably larger. So even our sobering 67-MW power estimate was overly optimistic. A later study indicated the actual power would be more like 500 MW.

For this design we added only the amount of memory that we thought we could afford

Next Generation Super Computers

without the power requirements of connecting it all together becoming too much of an issue. The resultant amount of memory, about 3.6 petabytes in all, seems large at first blush, but it provides far less memory than the 1 byte per flops that is the supercomputer designer's holy grail. So unless memory technologies emerge that have greater densities at the same or lower power levels than we assumed, any exaflops-capable supercomputer that we sketch out now will be memory starved.

And we're not even done with the seemingly insurmountable obstacles!

Supercomputers need long-term storage that's dense enough and fast enough to hold what are called checkpoint files. These are copies of main memory made periodically so that if a fault is discovered, a long-running application need not be started over again from the beginning. The panel came to the conclusion that writing checkpoint files for exaflops-size systems may very well require a new kind of memory entirely, something between DRAM and rotating disks. And we saw very limited promise in any variation of today's flash memory or in emerging nanotechnology memories, such as carbon nanotubes or holographic memory.

As if the problems we identified with excessive power draw and memory inadequacies weren't enough, the panel also found that lowering the operating voltage, as we presumed was necessary, would make the transistors prone to new and more-frequent faults, especially temperature-induced transient glitches. When you add this tendency to the very large number of components projected—more than 4 million chips with almost a billion chip contacts—you have to worry about the resiliency of such systems. There are ways to address such concerns, but most solutions require additional hardware, which increases power consumption even further.

So are exaflop computers forever out of reach? I don't think so. Meeting DARPA's ambitious goals, however, will require more than the few short years we have left before 2015. Success in assembling such a machine will demand a coordinated cross-disciplinary effort carried out over a decade or more, during which time device engineers and computer designers will have to work together to find the right combination of processing circuitry, memory structures, and communications conduits—something that can beat what are normally voracious power requirements down to manageable levels.

Next Generation Super Computers

Also, computer architects will have to figure out how to put the right kinds of memory at the right places to allow applications to run on these systems efficiently and without having to be restarted constantly because of transient glitches. And hardware and software specialists will have to collaborate closely to find ways to ensure that the code running on tomorrow's supercomputers uses a far greater proportion of the available computing cores than is typical for supercomputers today.

That's a tall order, which is why I and the other DARPA panelists came away from the study rather humbled. But we also found a greater understanding of the hurdles, which will shape our research for many years to come. I, for example, am now exploring how new memory technologies can reduce the energy needed to fetch data and how architectures might be rearranged to move computation to the data rather than having to repeatedly drag copies of that data all around the system.

Perhaps more important, government funding agencies now realize the difficulties involved and are working hard to jump-start this kind of research. DARPA has just begun a program called Ubiquitous High Performance Computing. The idea is to support the research needed to get both very compact high-performance computers and rack-size supercomputers built, even if bringing a warehouse full of them together to form a single exaflops-class machine proves to be prohibitive. The hope is to be able to pack something equivalent to today's biggest supercomputers into a single truck, for example. The U.S. Department of Energy and the National Science Foundation are funding similar investigations, aimed at creating supercomputers for solving basic science problems.

So don't expect to see a supercomputer capable of a quintillion operations per second appear anytime soon. But don't give up hope, either. If rack-size high-performance computers do indeed become as ubiquitous as DARPA's new program name implies they will, a widely distributed set of these machines could perhaps be made to work in concert. As long as the problem at hand can be split up into separate parts that can be solved independently, a colossal amount of computing power could be assembled—similar to how cloud computing works now. Such a strategy could allow a virtual exaflops supercomputer to emerge. It wouldn't be what DARPA asked for in 2007, but

Next Generation Super Computers

for some tasks, it could serve just fine.

This article originally appeared in print as "The Tops in Flops."

About the Author

Peter Kogge, an IEEE Fellow, is a professor of computer science and engineering at the University of Notre Dame, where he also holds an appointment in the department of electrical engineering. While at IBM in the 1970s, he worked on the space shuttle's input/output processor and on the IBM 3838 Array Processor, which was the fastest single-precision floating-point processor the company sold at the time. "Today your cellphone probably has an order of magnitude more computing power," says Kogge."

The Next Graphene?

The Next Graphene?

Two-dimensional sheets of molybdenite can do something that graphene can't.

By Katherine Bourzac

Molybdenite, a mineral that's currently used as a lubricant, turns out to have extraordinary electronic properties when deposited in single-atom-thick strips. Researchers in Switzerland have now made high-performance transistors out of this form of molybdenite. Used in this way, the mineral could hold promise for more efficient flexible solar cells, electronics, or high-performance digital microprocessors.

Like graphene, an atom-thick form of carbon, "two-dimensional" molybdenite has electrical and optical properties that are much better than those found in three-dimensional forms of the material.

Researchers led by **Andras Kis** at the École Polytechnique Fédérale de Lausanne (EPFL) made molybdenite transistors using methods used in the early days of graphene research. Molybdenite, a relatively inexpensive mineral of molybdenum disulfide, has a layered structure similar to that of raw graphite. Kis's group crushed crystals of molybdenite between folded pieces of tape, peeling back layer after layer until all that remained were single-atom-thick sheets. They then deposited the molybdenite sheets onto a substrate, added a layer of insulating material, and used standard lithography to add source and drain electrodes and a gate to make a transistor. Other researchers had done this before but didn't get good performance. Kis says the molybdenite transistors have a comparable electrical mobility to similar ones made from graphene nanoribbons.

After Andre Geim and Kostya Novoselov demonstrated the promise of graphene in 2004—a feat that won them the **Nobel Prize** in 2010—there was a burst of interest in making and testing other two-dimensional materials. But graphene was considered more promising than anything else, and other materials came to be seen as curiosities, says **James Hone**, professor of mechanical engineering at Columbia University. Hone was part of a group that demonstrated that graphene is the **strongest material ever** tested. Hone, who is not affiliated with the EPFL researchers, expects their results to generate new interest in other two-dimensional materials, and molybdenite in particular. "This is a very promising result that will make us look at this material more carefully and see how we can squeeze better performance out of it," he says.

Importantly, molybdenite is a semiconductor, which means it provides discrete energy levels for electrons to jump through—a property known as its bandgap. This is key for

The Next Graphene?

any material used in a digital transistor. Graphene does not have a bandgap, and to give it one, researchers must layer it or cut it into ribbons, which is complex and can lead to the degradation of graphene's other properties. "You have to work very hard to open up a bandgap in graphene," says **James Tour**, professor of chemistry and computer science at Rice University.

Graphene was originally seen as a material that could replace silicon in digital logic circuits, the type at the heart of today's microprocessors. But because it's so hard to make it into a semiconductor, it's becoming clear that graphene's promise lies elsewhere, for example in superfast analog circuits, the type used for telecommunications and radar, says **Phaedon Avouris**, who leads the IBM group developing graphene electronics. Molybdenite's bandgap is particularly promising for solar cells, LEDs, and other electro-optical devices.

But this is not enough for a material to show promise for digital logic, cautions Avouris. Molybdenite's properties must be further demonstrated before people in the electronics industry can get excited about it, he says. Researchers will also have to show, for example, that molybdenite has the properties necessary to significantly amplify electrical signals. "It's too early to say how promising this is," Avouris cautions.

Even before molybdenite's promise for high-performance microprocessors is proven—or isn't—researchers expect to find other uses for it. "You can buy metric tons of this stuff," says Hone. He points to work on making liquid suspensions of molybdenite sheets, which might be practical for making flexible solar cells and other electronics—the manual peeling method Kis used isn't practical for making large volumes of devices. "Typically, flexible electronics use polymers, but molybdenite would be more stable," he predicts.

Kis hopes that his results will encourage chemists to work on the problem of producing molybdenite sheets, as Geim and Novoselov's work encouraged people to work on methods for making large amounts of graphene. "To be promising for industry, you need to have some large-scale synthesis method for making a material," says Avouris. "It's the same problem there was in the beginning with graphene."

Tour says that Kis's results will indeed encourage chemical engineers to jump in and work with molybdenite. He says that the first experiments with graphene did not fully demonstrate its promise—researchers didn't know how to work with it. After years of working with graphene, chemists should be better able to work with molybdenite. "You already have a sense of how to handle it. This will be greatly benefited by the work

The Next Graphene?

we've been doing with graphene," Tour says.

Carnegie Mellon Assisting IBM's "Watson" with Machine Learning

CMU and IBM Collaborate on Open Computing System For Advancing Research on Question Answering

"Watson" To Play "Jeopardy!" Champions, Feb. 14-16

Professor Eric Nyberg and his Ph.D. students, Nico Schlaefer and Hideki Shima, discuss the Watson project.

PITTSBURGH—Carnegie Mellon University today announced that it is one of eight universities collaborating with IBM to advance the Question Answering (QA) technology behind the IBM "Watson" computing system.

IBM and CMU have collaborated on the Open Advancement of Question-Answering Initiative (OAQA), which encouraged the creation of a computer architecture and methodologies that could be used by researchers to support the Watson system. Watson will compete against "Jeopardy!" champions Ken Jennings and Brad Rutter in a historic "man vs. machine" match that will air on Jeopardy! Feb. 14-16.

"IBM Watson is the first step in how computers will be designed and built differently and will be able to learn, and with the help of Carnegie Mellon we will continue to advance the QA technologies that are the backbone of this system," said David Ferrucci, leader of the IBM Watson project team.

"The idea that a person could ask a computer a question in standard English and get a specific, accurate and authoritative answer has fired imaginations since the beginning of the computer age," said Eric Nyberg, a professor in CMU's Language Technologies Institute. "Despite years of work, major advances in transforming this from science fiction into reality have taken too long. That's why Carnegie Mellon and IBM together developed this approach we call Open Advancement of Question Answering."

The OAQA approach includes a modular software architecture and a common set of measurement standards. This enables researchers to test software components they have developed for specific QA tasks in a way that allows a direct comparison with the components of other researchers. This approach, which IBM used as it designed Watson, also allows individual components in the system to be easily swapped out or upgraded as necessary.

"With OAQA, researchers no longer have to reinvent the wheel every time they develop a new QA system," Nyberg said. QA systems are complex,

Carnegie Mellon Assisting IBM's "Watson" with Machine Learning

requiring software components for deciphering natural language, for searching through text documents and for formulating and evaluating potential answers. "In the past, it's been all but impossible to determine the individual performance of these software components. And it's been difficult for researchers to build on the success of others by simply plugging in the best available component into their own system. OAQA changes all of that," he said.

In addition to IBM and CMU, researchers at the Massachusetts Institute of Technology, the University of Texas at Austin, the University of Southern California, Rensselaer Polytechnic Institute, SUNY Albany, the University of Trento and the University of Massachusetts Amherst have participated in the OAQA Initiative. The elements of OAQA are open source and available for download from the OAQA website, <http://mu.lti.cs.cmu.edu/trac/oaqa>.

"We are glad to be collaborating with such distinguished universities and experts in their respective fields who can contribute to the advancement of QA technologies that help enable the Watson system," IBM's Ferrucci said. "The success of the Jeopardy! challenge will break barriers associated with computing technology's ability to process and understand human language, and will have profound effects on science, technology and business."

Computer scientists have been designing QA systems for 50 years and IBM and Carnegie Mellon have long been collaborators. This relationship began in 2001, with a federally sponsored program called Advanced Question Answering for Intelligence (AQUAINT). AQUAINT included an investigation of software architectures and tools that could be of general benefit to QA researchers. This sparked an ongoing IBM-CMU collaboration on the development and dissemination of the Unstructured Information Management Architecture (UIMA), an open-source software library that has become a fundamental part of QA systems developed at CMU and IBM.

In 2007, Nyberg and his Ph.D. students, Nico Schlaefer and Hideki Shima, began working with IBM on the Watson project. Realizing that success with Watson could spur new QA research and also support new business applications, IBM and Carnegie Mellon began pioneering the development of OAQA in 2008. Nyberg, Schlaefer and Shima discuss Watson and their contributions on this video, <http://www.youtube.com/watch?v=ls2IgNiOftA>.

Jeopardy! questions are just one type of QA task. In contrast to general

Carnegie Mellon Assisting IBM's "Watson" with Machine Learning

keyword search engines such as Google or Bing, QA systems are designed to provide useful answers to specific questions posed by people using their everyday language. Jeopardy! probes general knowledge and places a premium on speed, but other systems can be configured to provide information about a specific range of products or to provide deep answers to questions on highly technical or legally complex subjects.

The OAQA approach is being used in a Machine Reading project sponsored by the Defense Advanced Research Projects Agency that began last year. IBM, the prime contractor, is working with Carnegie Mellon, the University of Texas at Austin, the University of Southern California and the University of Utah to develop a universal text engine that captures information from natural language texts and stores it in a knowledge base that can be readily accessed by QA and other computer systems.

What IBM's Watson Tells Us About the State of AI

What IBM's Watson tells us about the state of AI

by [Gordon Haff](#)

Computers that reliably understand human communications have been a staple of fiction going back decades or more. The Enterprise's computer in the 1960s vintage "Star Trek" series is as good an example as any. And truth is, that particular science-fictional ability probably would not have seemed all that remarkable to the typical person of the time.

Access billions of pages of text, pictures, and video from a gadget I can fit in my pocket? Play a game with immersive graphics on a huge, high-resolution screen that hangs on the wall? For a computer engineer, the fact that those inexpensive consumer devices have more computing power than all the then-computers in the world would impress as well. But understanding speech? That's something a toddler can do.

But understanding speech has turned out to be really difficult. In fact, just converting speech to text has been a huge challenge. Indeed, when [IBM Watson takes on past "Jeopardy" champions](#) in a [contest televised beginning tonight](#), the questions will be fed to it as text, rather than speech. But answering the often convoluted questions used on "Jeopardy" is hard enough even without processing the spoken word.

Although this contest takes place in the artificial setting of a game show, it does give us a glimpse into what is possible and what is not with artificial intelligence, that is AI, today. And perhaps where AI is going.

AI research is generally considered to have launched in 1956 at the Dartmouth Summer Research Conference on Artificial Intelligence. The hope of many researchers at that time was that they would be able to create a so-called "strong AI" over the next few decades--which is to say an AI that could reason, learn, plan, and communicate. Research in this vein has produced very limited results. One of the big problems has been the almost equal lack of progress in understanding how humans think. Thus, the failure of strong AI may well be related to the equal lack of progress in significant areas of cognitive psychology.

Some of the AI pioneers still have a more optimistic view. MIT's Marvin Minsky places the blame more on a shift away from fundamental research. As he puts it, "The great laboratories somehow disappeared, economies became tighter, and companies had to make a profit--they couldn't start projects that would take 10 years to pay off."

So Watson is in no real sense thinking and the use of the term "understanding" in the context of Watson should be taken as anthropomorphism rather than a literal description.

Is Watson just about brute force then? One might think so. [Its hardware specs are impressive](#): IBM Watson is comprised of ninety IBM POWER 750 servers, 16 Terabytes of memory, and 4 Terabytes of clustered storage. This is enclosed in ten racks including the servers, networking, shared disk system, and cluster controllers. These ninety POWER 750 servers have four POWER7

What IBM's Watson Tells Us About the State of AI

processors, each with eight cores. IBM Watson has a total of 2880 POWER7 cores.

To put this in perspective, by my estimate, Watson would have been the fastest supercomputer in the world on the TOP500 list [just five years ago](#). And, although the disk and memory specs aren't nearly so impressive, remember that we're just talking about text-based data here. In fact, it's loaded with [millions of documents](#)--making the fact that it, like the human contestants, isn't hooked up to the Internet something of a red herring.

Chris Anderson, the editor in chief of Wired, argues that [data often replaces underlying theory](#). He goes on to quote Peter Norvig, Google's research director: "All models are wrong, and increasingly you can succeed without them."

But thinking of Watson as just a big, fast computer that just points to Wikipedia or the Oxford English dictionary and the right answer pops out understates the complexity of the natural language processing that has to go on. If Jeopardy consisted solely of grade-school type questions--excuse me, answers--like "the 42nd president of the United States," this would in fact be a relatively simple exercise. But many Jeopardy questions consist of wordplay, riddles, and other barriers to literal lookup of answers.

Watson is part of IBM's DeepQA project. The QA stands for question answering. [As IBM researchers put it:](#)

the open-domain QA problem is attractive as it is one of the most challenging in the realm of computer science and artificial intelligence, requiring a synthesis of information retrieval, natural language processing, knowledge representation and reasoning, machine learning, and computer-human interfaces.

In association with Carnegie Mellon University, IBM created the Open Advancement of Question Answering (OAQA) initiative "to provide a foundation for effective collaboration among researchers to accelerate the science of automatic question answering." Among other things, this initiative is intended to enable adapting Watson's software to new data domains and problem types.

Although Watson is certainly a powerful computer loaded with lots of data, [as described in this PBS video](#), the software is very much a key ingredient here; many new algorithms and approaches were needed to make Watson competitive with strong human players. For example, to learn from examples, to understand how context affects the significance of names and places, and to correlate multiple facts in a particular answer.

Strong AI proponents may well view something like Watson as something of a parlor trick in that it doesn't really try to reason as a human does. But, that said, there's much more--dare we say intelligence--involved here than there is in playing chess, a well-bounded and formalized problem. And given the longtime difficulty of understanding real intelligence, this is the AI path that seems to hold the most promise for now.

A Fight to Win the Future: Computers vs. Humans

A Fight to Win the Future: Computers vs. Humans

By **JOHN MARKOFF**

STANFORD, Calif. — At the dawn of the modern computer era, two Pentagon-financed laboratories bracketed [Stanford University](#). At one laboratory, a small group of scientists and engineers worked to replace the human mind, while at the other, a similar group worked to augment it.

In 1963 the mathematician-turned-computer scientist John McCarthy started the Stanford Artificial Intelligence Laboratory. The researchers believed that it would take only a decade to create a thinking machine.

Also that year the computer scientist Douglas Engelbart formed what would become the Augmentation Research Center to pursue a radically different goal — designing a computing system that would instead “bootstrap” the human intelligence of small groups of scientists and engineers.

For the past four decades that basic tension between artificial intelligence and intelligence augmentation — A.I. versus I.A. — has been at the heart of progress in computing science as the field has produced a series of ever more powerful technologies that are transforming the world.

Now, as the pace of technological change continues to accelerate, it has become increasingly possible to design computing systems that enhance the human experience, or now — in a growing number of cases — completely dispense with it.

The implications of progress in A.I. are being brought into sharp relief now by the broadcasting of a recorded competition pitting [the I.B.M. computing system named](#)

A Fight to Win the Future: Computers vs. Humans

Watson against the two best human Jeopardy players, Ken Jennings and Brad Rutter.

Watson is an effort by I.B.M. researchers to advance a set of techniques used to process human language. It provides striking evidence that computing systems will no longer be limited to responding to simple commands. Machines will increasingly be able to pick apart jargon, nuance and even riddles. In attacking the problem of the ambiguity of human language, computer science is now closing in on what researchers refer to as the “Paris Hilton problem” — the ability, for example, to determine whether a query is being made by someone who is trying to reserve a hotel in France, or simply to pass time surfing the Internet.

If, as many predict, Watson defeats its human opponents on Wednesday, much will be made of the philosophical consequences of the machine’s achievement. Moreover, the I.B.M. demonstration also foretells profound sociological and economic changes.

Traditionally, economists have argued that while new forms of automation may displace jobs in the short run, over longer periods of time economic growth and job creation have continued to outpace any job-killing technologies. For example, over the past century and a half the shift from being a largely agrarian society to one in which less than 1 percent of the United States labor force is in agriculture is frequently cited as evidence of the economy’s ability to reinvent itself.

That, however, was before machines began to “understand” human language. Rapid progress in natural language processing is beginning to lead to a new wave of automation that promises to transform areas of the economy that have until now been untouched by technological change.

A Fight to Win the Future: Computers vs. Humans

“As designers of tools and products and technologies we should think more about these issues,” said Pattie Maes, a computer scientist at the [M.I.T. Media Lab](#). Not only do designers face ethical issues, she argues, but increasingly as skills that were once exclusively human are simulated by machines, their designers are faced with the challenge of rethinking what it means to be human.

I.B.M.’s executives have said they intend to commercialize Watson to provide a new class of question-answering systems in business, education and medicine. The repercussions of such technology are unknown, but it is possible, for example, to envision systems that replace not only human experts, but hundreds of thousands of well-paying jobs throughout the economy and around the globe. Virtually any job that now involves answering questions and conducting commercial transactions by telephone will soon be at risk. It is only necessary to consider how quickly A.T.M.’s displaced human bank tellers to have an idea of what could happen.

To be sure, anyone who has spent time waiting on hold for technical support, or trying to change an airline reservation, may welcome that day. However, there is also a growing unease about the advances in natural language understanding that are being heralded in systems like Watson. As rapidly as A.I.-based systems are proliferating, there are equally compelling examples of the power of I.A. — systems that extend the capability of the human mind.

[Google](#) itself is perhaps the most significant example of using software to mine the collective intelligence of humans and then making it freely available in the form of a digital library. The search engine was originally based on a software algorithm called PageRank that mined human choices in picking Web pages that contained answers to a

A Fight to Win the Future: Computers vs. Humans

particular typed query and then quickly ranked the matches by relevance.

The Internet is widely used for applications that employ a range of human capabilities. For example, experiments in [Web-based games](#) designed to harness the human ability to recognize patterns — which still greatly exceeds what is possible by computer — are generating a new set of scientific tools. Games like FoldIt, EteRNA and Galaxy Zoo make it possible for individuals [to compete and collaborate](#) in fields like astronomy to biology, medicine and possibly even material science.

Personal computing was the first step toward intelligence augmentation that reached a broad audience. It created a generation of “information workers,” and equipped them with a set of tools for gathering, producing and sharing information. Now there is a cyborg quality to the changes that are taking place as personal computing has evolved from desktop to laptop and now to the smartphones that have quickly become ubiquitous.

The smartphone is not just a navigation and communication tool. It has rapidly become an almost seamless extension of almost all of our senses. It is not only a reference tool but is quickly evolving to be an “information concierge” that can respond to typed or spoken queries or simply volunteer advice.

Further advances in both A.I. and I.A. will increasingly confront the engineers and computer scientists with clear choices about how technology is used. “There needs to be an explicit social contract between the engineers and society to create not just jobs but better jobs,” said Jaron Lanier, a computer scientist and author of “You are not a Gadget: A Manifesto.”

A Fight to Win the Future: Computers vs. Humans

The consequences of human design decisions can be clearly seen in the competing online news systems developed here in Silicon Valley.

Each day Katherine Ho sits at a computer and observes which news articles millions of [Yahoo](#) users are reading.

Her computer monitor displays the results of a cluster of software programs giving her almost instant updates on precisely how popular each of the news articles on the company's home page is, based on her readers' tastes and interests.

Ms. Ho is a 21st-century version of a traditional newspaper wire editor. Instead of gut and instinct, her decisions on which articles to put on the [Yahoo home page](#) are based on the cues generated by the software algorithms.

Throughout the day she constantly reorders the news articles that are displayed for dozens of demographic subgroups that make up the Yahoo readership. An article that isn't drawing much interest may last only minutes before she "spikes" it electronically. Popular articles stay online for days and sometimes draw tens of millions of readers.

Just five miles north at Yahoo's rival Google, however, the news is produced in an entirely different manner. [Spotlight](#), a popular feature on Google's [news site](#), is run entirely by a software algorithm which performs essentially the same duties as Ms. Ho does.

Google's software prowls the Web looking for articles deemed interesting, employing a process that is similar to the company's PageRank search engine ranking system to make

A Fight to Win the Future: Computers vs. Humans

decisions on which articles to present to readers.

In one case, software-based technologies are being used to extend the skills of a human worker, in another case technology replaces her entirely.

Similar design decisions about how machines are used and whether they will enhance or replace human qualities are now being played out in a multitude of ways, and the real value of Watson may ultimately be in forcing society to consider where the line between human and machine should be drawn.

Indeed, for the computer scientist John Seely Brown, machines that are facile at answering questions only serve to obscure what remains fundamentally human.

“The essence of being human involves asking questions, not answering them,” he said.

For Watson Technology, What Happens After 'Jeopardy!'?

For Watson Technology, What Happens After 'Jeopardy!'?

IBM's Supercomputer Has Implications for Healthcare, Information Tech and More

"Dealing with natural language is a very, very hard task for a computer," Ferrucci said. "But then, moreover, there's tremendous potential if we can continue to chip away at this task."

In medicine, for example, a [Watson](#)-like system could serve as a kind of doctor's assistant, he said.

Let's say a patient suffers from a rare disease, the medical Watson could listen in on patient interviews and combine those conversations with the patient's medical record, family history and test results. Not only that, but it could cross-reference that material against relevant journal articles, research and other published information.

Applications of Watson Technology Could Extend to Government, Engineering

Finally, it could generate a list of the top conditions the patient might be suffering from, along with a list of all the relevant sources.

"What the doctor can do is just consult this and say, am I missing anything? There's a huge amount of information out there," Ferrucci said. "I imagine that it will help the doctor to adjust and refine and rationalize and document both the diagnostic process as well as the treatment process with a lot more confidence."

Watson-like systems may not be as precise as a rule-based system working over a specific database, he said, but they can cover a wider collection of information and then make it more digestible for humans.

Ferrucci said the same process could be used by information technology professionals to unravel complicated computer problems.

IBM's immediate challenge might be to best world-champions on "Jeopardy!," but, ultimately, the company is looking to apply Watson's technology to areas as varied as government, engineering and business.

'Jeopardy!' Challenge Could Spark Public Conversation, Drive Research

Eric Nyberg, a professor in the Language Technologies Institute at Carnegie Mellon University, said he hopes the "[Jeopardy!](#)" competition will not only open up a

For Watson Technology, What Happens After 'Jeopardy!'?

conversation with the public about artificial intelligence, but also drive more research in the field.

As far as consumer applications, he said, "I think the logical next step beyond Watson is going to be systems that can advise you on selecting certain kinds of products that meet your personal needs."

For example, we may not be too far away from a system that could read through all the camera reviews available and then, based on its knowledge of a user's preferences, recommend the best choices, Nyberg said.

The system could be accessed in a retail shop where you would buy the camera, but it could also be accessible through a cell phone, he said.

"We could build applications like that today. For example, if there was a manufacturer that wanted to create a version of Watson that could answer questions about its entire product line that would be a very easy thing to do," he said, adding that the range of trivia and language used in "Jeopardy!" actually poses a more difficult problem.

But though Watson may represent a ground-breaking step in so-called question-answering systems, researchers say it's still not the ultimate goal in artificial intelligence.

Goal of AI: Build Machines With Human Intelligence

"From the science point of view, the goal of artificial intelligence, when it started 50 years ago was to build machines that exhibit human intelligence," said Boris Katz, the principal research scientist at MIT's Computer Science and Artificial Intelligence Laboratory. "One could argue that answering certain questions is part of that but I think it would be especially interesting to build something that not only performs certain tasks but maybe even does it in a way that a human would do it."

Those machines would not just provide answers to questions, but be able to explain how they arrived at the correct answer. And, given the trend toward mobile devices, he said, eventually, those machines will likely find their way into your hands.

Some smartphone applications can already understand limited voice commands and execute basic tasks like dialing contacts in your phone book but, Katz said, advanced systems could potentially turn your computer into a hand-held buddy.

"Your pocket friend -- more than Watson," he said. "Not only [to] answer simple questions, but actually do things. ... [You could instruct it to] 'Please tell my friend to do this,' 'please find this information and summarize it'."

For Watson Technology, What Happens After 'Jeopardy!'?

That scenario is probably still decades away, he said, but it starts with the natural language research that put Watson on "Jeopardy!".

So while you might want to be loyal and root for the human race next week, the future may not be such a bad consolation prize if man ultimately does get defeated by machine.

Laser-Quick Data Transfer

Laser-Quick Data Transfer

Researchers learn how to make lasers directly on microchips—the result could be computers that download large files much more quickly.

By Katherine Bourzac

For the first time, researchers have grown lasers from high-performance materials directly on silicon. Bringing together electrical and optical components on computer chips would speed data transfer within and between computers, but the incompatibility of the best laser materials with the silicon used to make today's chips has been a major hurdle.

By growing nanolasers made of so-called exotic semiconductors on silicon, researchers at the University of California, Berkeley, have surmounted this hurdle. With further development, the Berkeley lasers could provide ways to transfer more data more quickly, speeding up computing within supercomputers and making it faster to download large files.

"Getting data on and off your laptop is becoming a bottleneck," says **Mario Paniccia**, director of Intel's Photonics Technology Lab. It's difficult to push data through today's copper wiring at rates higher than 10 gigabits per second. This slows data transfer between components of a computer, such as the CPU and the memory, and imposes limitations on design. Designers must put components as close together as possible so that data doesn't have to travel too far, generating heat and slowing down the system.

Data encoded in light pulses can travel farther faster and with lower losses. But the only way to get optical components onto today's chips is to do it using materials and manufacturing methods that are compatible with the silicon systems used in today's fabs. "The future of photonics is based on silicon," says **John Bowers**, Kavli chair of nanotechnology at the University of California, Santa Barbara. The problem is that silicon itself is a poor laser material, wasting a lot of energy and making little light.

The most efficient lasers are made out of a group of materials called "III-V" semiconductors, whose numerical name comes from the columns of the periodic table where the elements used to make them are found. Like silicon, these materials are crystalline. But the crystal lattices of silicon and of these materials do not line up with one another because the atoms are different sizes. When researchers grow III-V materials on top of silicon, the III-V crystal strains to align with the silicon crystal, leading to defects that degrade performance.

Laser-Quick Data Transfer

Connie Chang-Hasnain, professor of electrical engineering and computer science at Berkeley, has overcome this incompatibility between silicon and laser materials by taking advantage of the properties of nanostructures and by carefully controlling the growth process. The Berkeley researchers start by placing a silicon substrate inside a chemical growth chamber, raising the temperature to 400 °C, and flowing in gases containing indium, gallium, and arsenide. By controlling the ratios of the gases and their flow rates, Chang-Hasnain has found, it's possible to direct the growth of these III-V materials so that it starts from a small point called a "seed." As an indium-gallium nanopillar sprouts up from the seed, it forms a defect-free crystal. The seed seems to protect the rest of the structure from the influence of the underlying silicon. The researchers then flow in a second set two gases to make a gallium-arsenide shell around the pillar.

When the nanopillar is pumped with light from another laser, the light spirals around inside the pillar, as if running up and down a spiral staircase. The difference in materials between the core and the shell encourages this effect, trapping the photons in this spiral until they reach a high enough energy threshold and are emitted. This spiraling effect is something that hasn't been seen in other types of lasers before. These results are described in the journal *Nature Photonics*. The next step is to demonstrate that the laser can be pumped with electrical energy, key to making a compact laser. Chang-Hasnain is confident the Berkeley researchers will make an electrically pumped laser. In another publication in *Nano Letters* her group demonstrated exotic semiconductor diodes on silicon, which they're now adapting to pump the nanolasers.

Another key to making lasers on silicon chips is not to let the temperature get too high. Chang-Hasnain says that her process could eventually be used to grow high-quality lasers on otherwise finished silicon chips patterned with transistors and optical components, giving them the capability of encoding data into pulses of light. Depositing high-quality III-V semiconductor crystals usually requires higher temperatures—instead of 400 °C, these materials are usually grown at 700 °C, a temperature that would destroy a microprocessor. Chang-Hasnain says it's the nanostructure of the lasers that makes this possible: high-quality nanostructures can generally be grown at lower temperatures than large films made from the same materials.

"A lot of progress has been made on silicon optical components," says Intel's Paniccia. However, progress on lasers that are compatible with silicon chips has lagged behind. Researchers have made various optical components from silicon using materials and processes already present in chip-manufacturing lines. But they have to add on the

Laser-Quick Data Transfer

lasers afterward. Intel, IBM, and other companies have been developing such workarounds.

Chang-Hasnain acknowledges that the group has many more things to prove, from electrical pumping of the lasers to proving they provide enough light of the right wavelengths and can couple it to other optical components. But Intel's Paniccia says the demonstration that these laser materials can be made compatible with silicon is "a big step."

Katherine Bourzac is the materials science editor for Technology Review.

Copyright Technology Review 2011.

Stanford Researchers Develop Wireless Technology for Faster, More Efficient Communications Networks

Stanford researchers develop wireless technology for faster, more efficient communication networks

A new technology that allows wireless signals to be sent and received simultaneously on a single channel has been developed by Stanford researchers. Their research could help build faster, more efficient communication networks, at least doubling the speed of existing networks.

Jack Hubbard

The technology could have some very practical applications, including better wireless reception.

BY SANDEEP RAVINDRAN

"Wireless communication is a one-way street. Over."

Radio traffic can flow in only one direction at a time on a specific frequency, hence the frequent use of "over" by pilots and air traffic controllers, walkie-talkie users and emergency personnel as they take turns speaking.

But now, Stanford researchers have developed the first wireless radios that can send and receive signals at the same time.

This immediately makes them twice as fast as existing technology, and with further tweaking will likely lead to even faster and more efficient networks in the future.

"Textbooks say you can't do it," said Philip Levis, assistant professor of computer science and of electrical engineering. "The new system completely reworks our assumptions about how wireless networks can be designed," he said.

Cell phone networks allow users to talk and listen simultaneously, but they use a work-around that is expensive and requires careful planning, making the technique less feasible for other wireless networks, including Wi-Fi.

Sparked from a simple idea

A trio of electrical engineering graduate students, Jung Il Choi, Mayank Jain and Kannan Srinivasan, began working on a new approach when they came up with a seemingly simple idea. What if radios could do the same thing our brains do when we listen and talk simultaneously: screen out the sound of

Stanford Researchers Develop Wireless Technology for Faster, More Efficient Communications Networks

our own voice?

In most wireless networks, each device has to take turns speaking or listening. "It's like two people shouting messages to each other at the same time," said Levis. "If both people are shouting at the same time, neither of them will hear the other."

It took the students several months to figure out how to build the new radio, with help from Levis and Sachin Katti, assistant professor of computer science and of electrical engineering.

Their main roadblock to two-way simultaneous conversation was this: Incoming signals are overwhelmed by the radio's own transmissions, making it impossible to talk and listen at the same time.

"When a radio is transmitting, its own transmission is millions, billions of times stronger than anything else it might hear [from another radio]," Levis said. "It's trying to hear a whisper while you yourself are shouting."

But, the researchers realized, if a radio receiver could filter out the signal from its own transmitter, weak incoming signals could be heard. "You can make it so you don't hear your own shout and you can hear someone else's whisper," Levis said.

Their setup takes advantage of the fact that each radio knows exactly what it's transmitting, and hence what its receiver should filter out. The process is analogous to noise-canceling headphones.

When the researchers demonstrated their device last fall at MobiCom 2010, an international gathering of more than 500 of the world's top experts in mobile networking, they won the prize for best demonstration. Until then, people didn't believe sending and receiving signals simultaneously could be done, Jain said. Levis said a researcher even told the students their idea was "so simple and effective, it won't work," because something that obvious must have already been tried unsuccessfully.

Breakthrough for communications technology

But work it did, with major implications for future communications networks. The most obvious effect of sending and receiving signals simultaneously is that it instantly doubles the amount of information you can send, Levis said. That means much-improved home and office networks that are faster and

Stanford Researchers Develop Wireless Technology for Faster, More Efficient Communications Networks

less congested.

But Levis also sees the technology having larger impacts, such as overcoming a major problem with air traffic control communications. With current systems, if two aircraft try to call the control tower at the same time on the same frequency, neither will get through. Levis says these blocked transmissions have caused aircraft collisions, which the new system would help prevent.

The group has a provisional patent on the technology and is working to commercialize it. They are currently trying to increase both the strength of the transmissions and the distances over which they work. These improvements are necessary before the technology is practical for use in Wi-Fi networks.

But even more promising are the system's implications for future networks. Once hardware and software are built to take advantage of simultaneous two-way transmission, "there's no predicting the scope of the results," Levis said.

Sandeep Ravindran is a science-writing intern at the Stanford News Service.

Researchers Detail Programmable Nanoprocessor

Researchers detail programmable nanoprocessor

By Jack Clark (@mappingbabel), ZDNet UK, 11 February, 2011 13:11

Topics

Researchers at Harvard University and the Mitre Corporation have detailed the architecture for a programmable nanoprocessor built out of ultra-small 'nanowires'.

The nanoprocessor, outlined in a *Nature* article published on Wednesday, is formed of 496 non-volatile field effect transistor (FET) nodes arranged in a 960-micrometre square area, overlaid with semiconductor materials.

Researchers at Harvard University and the Mitre Corporation have detailed the architecture for a programmable nanoprocessor built out of ultra-small 'nanowires'.

"This work represents a quantum jump forward in the complexity and function of circuits built from the bottom up," said Charles Lieber, who led the research, in a statement. "[The work] demonstrates that this bottom-up paradigm, which is distinct from the way commercial circuits are built today, can yield nanoprocessors and other integrated systems of the future."

Each [nanowire](#) is built from a 10-nanometre diameter germanium nanowire core and a two-nanometre thick silicon shell. The nanowires can be operated as individual transistors by passing current through metal wires woven through the layer of semiconductor materials above them.

“*This work represents a quantum jump forward in the complexity and function of*

Researchers Detail Programmable Nanoprocessor

circuits built from the bottom up. ”

– Charles Lieber, Harvard University

The nanowire transistors are non-volatile, so once their state has been defined by the passing of current through the semiconductor over-lattice they require no additional power to maintain memory. The researchers say in the *Nature* paper that the circuits do have limitations in comparison with industry-standard CMOS circuits, although projections suggest that the density, speed and power consumption can be further improved.

"Because of their very small size and very low power requirements, these new nanoprocessor circuits are building blocks that can control and enable an entirely new class of much smaller, lighter-weight electronic sensors and consumer electronics," said Shamik Das, lead engineer in Mitre's Nanosystems Group, in the statement.

One particular application would be for the use in embedded electronic systems and new types of therapeutic devices, according to *Nature*.

"This new nanoprocessor represents a major milestone toward realising the vision of a nanocomputer that was first articulated more than 50 years ago by physicist Richard Feynman," said James Ellenbogen, a chief scientist at Mitre, in the statement.

The Smallest Computing Systems Yet

The Smallest Computing Systems Yet

Nanowire transistors could run inside microscopic biosensors or environmental sensors.

By Kate Greene

A team led by [Charles Lieber](#), a professor of chemistry at Harvard, and Shamik Das, lead engineer in MITRE's nanosystems group, has designed and built a reprogrammable circuit out of nanowire transistors. Several tiles wired together would make the first scalable nanowire computer, says Lieber. Such a device could run inside microscopic, implantable biosensors, and ultra-low-power environmental or structural sensors, say the researchers.

For more than a decade, nanowires and nanotubes have promised to shrink computing to scales impossible to achieve with traditional semiconductor materials. But there have been doubts about the practicality of nanowires and nanotubes as actual computing systems. "There had been little progress in terms of increasing the complexity of circuits," says Lieber.

One big problem has been reproducing structures made from nanowires and nanotubes reliably. Each structure needs to be virtually identical to ensure that a circuit operates as intended. But now, says Lieber, some of those problems are being solved. His group, in particular, has developed ways to produce identical nanowires in bulk. Because of this, he and colleagues at MITRE have been able to design a nanowire circuit architecture that has the potential to scale up. The details are published in the current issue of *Nature*.

Traditional chips are made using a so-called top-down approach in which a design is essentially exposed like a photograph onto a semiconductor wafer, and excess material is etched away. In contrast, a bottom-up approach is used to make the nanowire circuits. This means they can be deposited on various types of surfaces, and can be made more compact. "You want [sensor] systems that are physically small," says James Klemic, nanotechnology laboratory director at MITRE. "Right now, your only option is to use a chip that dwarfs the sensor."

To make the new nanowire circuit, researchers deposited lines of nanowires, made of a germanium core and silicon shell, on a substrate and crossed them with lines of metal electrodes to create a grid. The points where the nanowires and electrodes intersect act as a transistor that can be turned on and off independently. The researchers made a single tile, with an area of 960 square microns containing 496

The Smallest Computing Systems Yet

functional transistors. It is designed to wire to other tiles so that the transistors, in aggregate, could act as complex logic gates for processing or memory.

The nanowire transistors maintain their state-on or off—regardless of whether the power is on. This gives it an instant-on capability, important for low-power sensors that might need to collect data only sporadically and also need to conserve power.

According to Das, the circuits could also be 10 times more power-efficient than circuits made of traditional materials. One reason is the nanowire's electrical properties, which don't allow electric current to leak, unlike traditional transistors. Another reason is that the circuit design uses capacitive connections instead of resistive ones, which are less efficient. "We don't burn a lot of power driving resistors," says Das.

"This is a significant milestone on several fronts," says [André DeHon](#), professor of electrical and system engineering at the University of Pennsylvania. Reprogrammable transistors made of nanowires are "the building block I was hoping for," he says.

The researchers' work represents "a leap forward in complexity and function of circuits built from the bottom up," says [Zhong Lin Wang](#), professor of materials science and engineering at Georgia Institute of Technology. It shows that the bottom-up method for manufacturing "can yield nanoprocessors and other integrated systems of the future," he says.

More work needs to be done to make nanowire processors practical for use in electronics systems, Lieber says. His group needs to demonstrate thousands of transistors on a tile—many times more than the current 496 transistors his group has so far achieved. In addition, they need to scale up to multiple tiles. The researchers are in the process of finding the best way to link a 16-tile system together. Lieber says that, realistically, manufacturing these circuits is still several years down the road.

Copyright Technology Review 2011.

New Anti-Laser Tech Paves Way for Optical Computing

New anti-laser tech paves way for optical computing

Device created by Yale researchers could be an integral element in optical computers that use light instead of electrons to process information

By Joab Jackson | IDG News Service

Yale University scientists have built what they call the first anti-laser, a device that can cancel out beams of light generated by a laser.

Such a device could be an integral element in optical computers, a long promised successor to today's computers that would use light instead of electrons to process information.

While scientists have long known of different ways to absorb light, this work is unique in that it can absorb light of a particular wavelength, the researchers claim.

"After some research, we found that several physicists had hinted at the concept in books and scientific papers, but no one had ever developed the idea," said Yale University physicist A. Douglas Stone, who along with fellow researcher Hui Cao led a team of researchers to build the anti-laser. The device was based on the theoretical work Stone published last summer. A summary of their work [appears](#) in the Feb. 18 issue of Science.

Lasers, short for Light Amplification by Stimulated Emission of Radiation, generate coherent light, which is to say a stream of light photons that all have [the same frequency, amplitude and wave pattern](#).

The researchers built what they call a Coherent Perfect Absorber (CPA), a silicon wafer that traps and dissipates incoming coherent light of a predefined wavelength. In other words, just as a laser generates coherent light, the CPA absorbs coherent light. The light's energy is dissipated as heat.

New Anti-Laser Tech Paves Way for Optical Computing

Such an anti-laser switch could help solve one of the toughest challenges in building an optical computer, namely the management and manipulation of the light used to encode information. For instance, a CPA could be used in an optical switch, one that would absorb light of a particular wavelength while letting light with other wavelengths pass. It could also be used to detect incoming light, or as a waveguide to direct beams of light along certain routes.

That could lead to optical switches replacing transistors in future computers. Optical computers could potentially be much more powerful than today's computers, given that the size of components could be shrunk beyond the limits of today's electron-based technologies.

As with any prototype, the CPA has some limitations, which the researchers feel can be overcome with more work. The current CPA absorbs 99.4 of all light it receives, but they would like to get that number up to 99.999 percent. Also the current CPA is one centimeter wide, which they say can be shrunk to a much more compact six microns.