

Index

Cyber Bytes - 18 APR 11

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

Links of interest:

ONR / Northrop Grumman Laser Demonstration: <http://www.youtube.com/usnavyresearch>

Cloud Computing

NSA Testing Smartphones, Tablets on Safe Mobile Architecture
- <http://www.nextgov.com/nextgov/ng_20110325_5941.php>

Why the Cloud Is Actually the Safest Place for Your Data
-<http://mashable.com/2011/03/29/cloud-computing-security/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Mashable+%28Mashable%29>

Cyber Security

Comodo Flap Highlights Browser Security Differences
- <http://news.cnet.com/8301-31921_3-20047729-281.html?part=rss&subj=news&tag=2547-1_3-0-20>

The RSA Attack: How They Did It
-<<http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/>>

Attack on RSA Used Zero-Day Flash Exploit in Excel
-<http://news.cnet.com/8301-27080_3-20051071-245.html?part=rss&subj=news&tag=2547-1_3-0-20>

An Attack Sheds Light on Internet Security Holes
-<http://www.nytimes.com/2011/04/07/technology/07hack.html?_r=1>

NASA Network Holes May Jeopardize Missions
- <http://news.cnet.com/8301-27080_3-20048540-245.html?part=rss&subj=news&tag=2547-1_3-0-20>

Microsoft Wins a Botnet Battle
-<<http://mobile.informationweek.com/10243/show/>>

Index

83ce6ee456f7dd5ce9a7a3dbbf112848/>

Social-media Tools Used to Target Corporate Secrets

-<<http://www.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm#>>

DHS Seeks to Grow Antibodies in Cyberspace

-<<http://www.fiercegovernmentit.com/story/dhs-seeks-grow-antibodies-cyberspace/2011-03-27>>

The Asymmetrical Online War

-<<http://bits.blogs.nytimes.com/2011/04/03/the-asymmetrical-online-war/>>

US Shatters Botnet, Can Disable Malware Remotely

-<http://news.cnet.com/8301-27080_3-20053708-245.html?part=rss&subj=news&tag=2547-1_3-0-20>

Malware Writers Making Code Tougher to Decode, Harder to Find

-<<http://www.darkreading.com/advanced-threats/167901091/security/application-security/229401546/malware-writers-making-code-tougher-to-decode-harder-to-find.html>>

US Shuts Down Massive Cyber Theft Ring

-<<http://us.mobile.reuters.com/article/topNews/idUSTRE73C7NQ20110413?irpc=932>>

US Law Enforcement Agencies Struggle to Detect Cyberattack Sponsors

-<http://www.nextgov.com/nextgov/ng_20110413_3265.php>

Busting the Botnets

-<<http://www.technologyreview.com/computing/37311/?ref=rss&a=f>>

Cyber War

New Pentagon Cyber Strategy Complete

Cyber Spending at Defense

-<http://www.nextgov.com/nextgov/ng_20110329_1325.php>

Virtual War a Real Threat

-<<http://www.latimes.com/news/nationworld/nation/la-na-cyber-war-20110328,0,1754694,full.story>>

Index

What a Cyber War with China Might Look Like

-<<http://www.computerworld.com/s/article/9215370/>

What_a_cyberwar_with_China_might_look_like>

Unconventional Methods Needed to Recruit Cyberwarriors

-<<http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=360>>

Iran Accuses Siemens Over Stuxnet Virus Attack

-<[http://www.reuters.com/article/2011/04/17/us-iran-nuclear-stuxnet-](http://www.reuters.com/article/2011/04/17/us-iran-nuclear-stuxnet-idUSTRE73G0NB20110417)

idUSTRE73G0NB20110417>

DOD

Federal IT Professionals to Receive New Program Manager Status

-<http://www.nextgov.com/nextgov/ng_20110330_3267.php>

Rapid Fielding Should Increase as Military Borrows from Private Sector

F-22s Won't Get F-35 Datalinks Yet

-<<http://www.dodbuzz.com/2011/03/31/f-22s-wont-get-f-35-datalinksyet/>>

Military Scouts Best Ways to Protect Stored Data

-<[http://defensesystems.com/articles/2011/03/29/cyber-defense-secure-data-storage-](http://defensesystems.com/articles/2011/03/29/cyber-defense-secure-data-storage-technologies.aspx)
technologies.aspx>

AirSea Battle Concept Is Focused on China

-<[http://www.aviationweek.com/aw/generic/story.jsp?id=news/awst/2011/04/04/
AW_04_04_2011_p62-299099.xml&headline=AirSea%20Battle%20Concept%20Is
%20Focused%20On%20China&channel=awst](http://www.aviationweek.com/aw/generic/story.jsp?id=news/awst/2011/04/04/AW_04_04_2011_p62-299099.xml&headline=AirSea%20Battle%20Concept%20Is%20Focused%20On%20China&channel=awst)>

'We're Not Gambling' [CNO on future of naval aviation; unmanned systems]

Soldiers' Wearable Computers May Get an iPhone Brain

-<[http://www.wired.com/dangerroom/2011/04/soldiers-wearable-computers-may-get-
an-iphone-brain/](http://www.wired.com/dangerroom/2011/04/soldiers-wearable-computers-may-get-an-iphone-brain/)>

Military Apps Putting iPhone in the Battlefield

-<[http://www.networkworld.com/news/2011/041411-military-iphone-apps.html?
hpg1=bn](http://www.networkworld.com/news/2011/041411-military-iphone-apps.html?hpg1=bn)>

DoD to Rewrite Acquisition Requirements Process [JCIDS Reform]

-<<http://www.defensenews.com/story.php?i=6236698&c=POL&s=TOP>>

Index

Defense Pursues 15-year Satellite Lease to Cut Battlefield Communications Costs
[DISA COMSAT Lease]

-<http://www.nextgov.com/nextgov/ng_20110414_5464.php>

Looking for IEDs? There's an app for that...

-<<http://blog.sei.cmu.edu/post.cfm/a-new-approach-for-handheld-devices-in-the-military>>

US Navy Getting Closer to Arming Ships with Lasers

-<http://news.cnet.com/8301-17938_105-20052949-1.html?part=rss&subj=news&tag=2547-1_3-0-20>

The Navy's Acquisitions Hiring Boom

-<<http://www.dodbuzz.com/2011/04/15/the-navys-acquisitions-hiring-boom/>>

Information & Society

US Products Help Block Mideast Web

- <<http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html?mod=djemalertNEWS>>

Engineering vs. Liberal Arts: Who's Right--Bill or Steve?

- <<http://techcrunch.com/2011/03/21/engineering-vs-liberal-arts-who's-right--bill-or-steve/>>

Information Technology

A Model for the Big Data Era

- <<http://www.informationweek.com/news/development/architecture-design/showArticle.jhtml?articleID=229301115>>

Microsoft Scheme Sniffs Out Unused Wireless Spectrum

- <<http://www.networkworld.com/news/2011/032511-usenix-microsoft-spectrum.html>>

Why Microsoft Struggles to Innovate (video): <http://money.cnn.com/video/technology/2011/03/28/ss_microsoft_herbold.fortune/>

Companies Hope to 'Program' the Internet

- <<http://www.technologyreview.com/computing/37226/page1/>>

Index

Microsoft, Google Spar Over Security Certification

-<http://news.cnet.com/8301-10805_3-20052815-75.html?part=rss&subj=news&tag=2547-1_3-0-20>

Robotics

Navy UCLASS Program to Develop Carrier-Based Unmanned Aircraft with Surveillance and Strike Capability by 2018

Military's Newest Recruit: C-3PO

-<<http://www.wired.com/dangerroom/2011/04/militarys-newest-recruit-c-3p0/>>

Navy Wants Unmanned 'Doc-Bots'

-<<http://www.wired.com/dangerroom/2011/04/navy-wants-doc-bots-robo-ambulances/>>

[Link to CMU research that is leading toward the Robo-Amubulances mentioned in the article: <http://www.fieldrobotics.org/cademo/>]

DARPA's Hologram Goggles Will Unleash Drone Hell

-<<http://www.wired.com/dangerroom/2011/04/holograms-bring-hell/>>

Space

Could 4G Wireless Plans Interfere with GPS?

-<<http://www.dodbuzz.com/2011/04/08/4g-wireless-could-interfere-with-gps/>>

Technology Advances

IBM's Watson Goes to College

-<<http://www.eweek.com/c/a/IT-Infrastructure/IBMs-Watson-Goes-to-College-306995/>>

IBM's Watson Not as Smart as You Think

-<http://www.computerworld.com/s/article/9215735/IBM_s_Watson_not_as_smart_as_you_think>

IBM Shows Smallest, Fastest Graphene Processor

-<http://www.computerworld.com/s/article/9215609/IBM_shows_smallest_fastest_graphene_processor>

US Navy's Laser Test Could Put Heat on Pirates

Index

-<http://news.yahoo.com/s/ap/20110413/ap_on_re_af/af_piracy_navy_laser>

Airborne Radar Will Map the Ground in 3D

-<<http://www.newscientist.com/article/mg21028065.300-airborne-radar-will-map-the-ground-in-3d.html>>

Batteries That Recharge in Seconds

-<http://www.technologyreview.com/printer_friendly_article.aspx?id=37324>

NSA Testing Smartphones, Tablets on Safe Mobile Architecture

[NSA testing smartphones, tablets on safe mobile architecture](#)

BY ALIYA STERNSTEIN 03/25/2011

The National Security Agency is testing a new mobile infrastructure, largely composed of commercial tools, to secure Top Secret information on portable devices, such as smartphones and tablet computers, a high-level NSA official said.

The intelligence community, like the rest of the federal workforce, increasingly wants to access information on the go, which is creating a challenge for Debora Plunkett, director of the NSA Information Assurance Directorate. Mobility is just one of about 10 challenges-- or "opportunities" as Plunkett likes to call them -- that she has set out to tackle this year, she said in an interview with *Nextgov*.

Moving ahead, her priority will remain bolstering national security networks at the agency responsible for safekeeping the nation's secrets and spying on others' covert activities, she said. But the evolving threat landscape has prompted her to change tactics.

After the disclosure of thousands of pages of classified material on the WikiLeaks website, there is increased interest in the data that NSA houses. In addition, technology is rapidly advancing, and cyber adversaries are becoming more sophisticated.

To shore up mobile devices, NSA is experimenting through the summer with an architecture comprised of commercial handsets and a data delivery concept similar to one used by Amazon's Kindle e-reader and OnStar Corp.'s navigation systems, Plunkett said. So-called mobile virtual network operators, or MVNOs, lease wireless capacity owned by other network providers, including Verizon Communications and Sprint, and then repackage the mobile services with their own specialized features under a new brand name, such as "OnStar."

But "the IT architecture of the future," said Plunkett, will be [cloud computing](#) --accessing over the Internet information technology systems that are grounded elsewhere-- and virtualization, a means of segmenting one physical server into smaller servers that can be accessed remotely.

Last week, U.S. Cyber Command chief Gen. Keith Alexander endorsed this sentiment when he testified before a House subcommittee that cloud computing will help fortify military networks during the coming year.

"This architecture would seem at first glance to be vulnerable to insider threats -- indeed, no system that human beings use can be made immune to abuse," he said, "but we are convinced the controls and tools that will be built into the cloud will ensure that people cannot see any data beyond what they need for their jobs and will be swiftly identified if they make unauthorized attempts to access

NSA Testing Smartphones, Tablets on Safe Mobile Architecture

data."

Both Plunkett and Alexander said they believe cloud computing will reduce security risks by moving information away from desktops to a centralized arrangement that allows for tighter control over access and more rapid responses to cyber incidents.

"We're tracking, absolutely," Plunkett said of their mutual goal. "I firmly believe that cloud computing is the way to go."

Like civilian agencies, NSA aims to continuously monitor its security posture by automating the process of collecting network status indicators, such as data on anti-virus scans or software patches, she added.

Other challenges this year include software assurance --the practice of making sure "the millions and millions and trillions of lines of code" that personnel exchange "is both developed securely and that it stays secure throughout its life cycle," Plunkett said.

Why the Cloud Is Actually the Safest Place for Your Data

Why the Cloud Is Actually the Safest Place for Your Data

17 hours ago by [Simon Crosby](#)

Simon Crosby is the CTO of the datacenter and cloud division at [Citrix Systems, Inc.](#) He was founder and CTO of XenSource prior to the acquisition of XenSource by Citrix. You can read more on his [blog](#) and also follow him on Twitter [@simoncrosby](#).

Worried about your data? If you're not, you're kidding yourself. It's become clear over the past few months that the risk of security breaches has reached a new and frightening level — from sophisticated tools in the hands of national governments and organized crime to spontaneous attacks harnessing the resources of thousands of loosely connected vigilantes. Add to that the dizzying array of devices now used to access, move and store data. Security strategies that seemed airtight only a few years ago now look like so much Swiss cheese.

In this light, your first instinct might be to pull back from cloud computing, viewing it as inherently less secure than keeping data and applications locked into hardware. After all, the word “cloud” itself implies that your precious assets are out there floating around somewhere, right? It's an understandable reaction and one that couldn't be more wrong. In fact, the cloud is now the safest place for your data.

Think about it: Data is lost when an organization loses control over it, including how it's stored, how it's transmitted, and what end users do with it. Clouds, and the virtualization technologies on which they run, give you back that control, from data center to delivery to endpoint.

Deliver User Experiences, Not Vulnerable Data

Why the Cloud Is Actually the Safest Place for Your Data

A key tenet of security is making sure data doesn't go astray when it leaves the enterprise. But what if data never left the enterprise in the first place? Desktop virtualization means that all data, applications and state remain centralized; users can access an immersive experience indistinguishable from traditional computing (actually even better in some regards, like instant-on apps) using either a hosted desktop or application experience, or a rich client experience. IT gains precise, granular control over applications and data. Everything is encrypted at rest, using keys that never leave the data center. Meanwhile, full back-end automation means less human involvement and less human involvement means less chance of things going wrong.

A locked down data center is all well and good, but how are workers supposed to be productive if they can't move data around? With virtualization, data is available from multiple points. Accordingly, there's never a reason to save anything to removable media (like the kinds that seem so often to fall into the wrong hands). A good desktop virtualization solution lets you set policies as to what kinds of client-side devices can be used, from thumb drives to printers.

What about offline use? No problem. Any data delivered to the desktop cache remains encrypted at all times, and IT holds the keys. Lost laptop? Disgruntled employee? Hotel room theft? Not to worry.

A New Perspective on Endpoint Security

A moment of silence, please: Traditional endpoint security is dead. It's simply no longer possible to detect attackers faster than they can mutate, and managing antivirus protection guest-by-guest can't possibly scale. It's also fundamentally incompatible with virtualization, since we can't have every endpoint in the organization trying to update a centralized attack file and index its virtual hard disk at the same time.

Why the Cloud Is Actually the Safest Place for Your Data

Symantec, it's time to rethink your business.

What if we take the reverse perspective? If we can't make data invulnerable, what if we make attacks less relevant by ensuring that each endpoint is in its best possible state? When a [hypervisor](#) is booted, one of the first things it does is check that it hasn't been modified since it was last signed by its creator. The same applies for each virtual machine. After each login, each VM is returned to its original state, so attackers have no way to gain a foothold in your environment. This approach — essentially, moving from blacklisting to whitelisting — is a fundamental shift in endpoint security.

There's still an important role for the security vendors to play in making virtual desktop security simpler and more scalable for large enterprise deployments, such as integrating in-hypervisor threat detection into both client-side and server-side virtualization products. Some of the top security providers are already doing exactly this, working in tandem with virtualization solution vendors. More will follow suit or find themselves stranded in an outdated and shrinking space.

Deny DoS Attacker

Even the best data security can't protect against a denial-of-service attack. You know what can? Truly massive perimeter control. But don't start pouring your own concrete yet. Why do you think people started keeping their money in a bank instead of at home? Because the bank has a better safe. So does Amazon. It's even better, as we've seen, than [PayPal](#) and [Visa](#). The largest cloud providers have defense resources far beyond anything you could match in your own datacenter.

Any way you look at it, the bottom line is clear: The online world may be getting more dangerous by the day — but the cloud is safer than ever.

Why the Cloud Is Actually the Safest Place for Your Data

Comodo Flap Highlights Browser Security Differences

March 28, 2011 4:15 AM PDT

Comodo flap highlights browser security differences

by [Declan McCullagh](#)

For all the tens of billions of dollars a year spent on Internet security a year, on everything from antivirus software to intrusion prevention, there's one component that's vital but remains obscure: which Web sites browsers decide to trust.

Each of the major browser makers has compiled a different list of who possesses the master keys to Web authentication--namely, who can be trusted to issue the secure digital certificates to create encrypted channels--and each has different procedures for approval. A closed lock icon typically appears in a browser and an "https://" connection is displayed when a Web site is deemed legitimate.

The flaws in this system were thrown into sharp relief by [last week's revelation](#) that a hacker traced to Iran obtained fake digital certificates for Google, Yahoo, Microsoft, and other companies. Comodo, a Jersey City, N.J.-based firm, said it [revoked the nine certificates](#) as soon as it discovered the breach in a business partner's systems.

Today's system gives browser makers tremendous responsibility. Any list of so-called certificate authorities they include will be trusted by billions of Web browsers around the world, unless users take the time to change the settings. The surprise is, perhaps, that the lists of who's trusted aren't the same.

"Microsoft appears to generally trust a much larger set of certificate authorities than Mozilla does," says [Peter Eckersley](#), senior staff technologist at the Electronic Frontier Foundation. "That may be because Microsoft's criteria are easier to meet in practice, or because certificate authorities prioritize getting onto Microsoft's list first."

Mozilla ships [Firefox](#) with a list of about 150 trusted certificate authorities. The [list](#) included with Microsoft Windows, used by Internet Explorer, totals 321 as of last week.

Opera includes only 37. Apple's OS X operating system, which [Safari](#) relies on, trusts 79 certificate authorities. Google says Chrome uses the Windows or OS X lists; Google Checkout trusts 168. (See CNET's [spreadsheet](#) with comparisons.)

It's difficult to compare those numbers directly, though, because some certificate authorities are counted multiple times. VeriSign appears 55 times in Microsoft's list based on different types of products offered but only once in Opera's, for instance.

Microsoft explicitly trusts more government-operated certificate authorities than any other browser maker. The list includes: Brazil, Hong Kong, India, Japan, Latvia, Lithuania, Serbia, Slovenia, the

Comodo Flap Highlights Browser Security Differences

United States, Tunisia, Turkey, Uruguay, and Venezuela.

Another complicating factor is that some browsers download updated lists of "root" certificate authorities as needed.

Opera's default "list starts out with a limited number of frequently used certificates," says [Yngve Pettersen](#), a senior developer at [Opera Software](#) in Oslo, Norway. "The remainder are downloaded as needed from [certs.opera.com](#) when the user actually visits a site issued from a root...We pre-ship some roots and also some intermediates, while others are downloaded dynamically."

What makes the list of trusted certificate authorities crucial is that each possesses the master keys to Web authentication. Companies like Etisalat, a wireless carrier in the United Arab Emirates that [implanted spyware](#) on customers' BlackBerry devices, can generate certificates that can be used to impersonate any secure Web site on the Internet. So do more than 100 German universities, the U.S. Department of Homeland Security, and random organizations like the Gemini Observatory, which operates a pair of 8.1-meter-diameter telescopes in Hawaii and Chile.

A fraudulent certificate would allow a network provider (or a government) to use what's known as a man-in-the-middle attack to impersonate the legitimate sites and grab passwords, read e-mail messages, and monitor any other activities on those Web sites, even if browsers show that the connections were securely protected with SSL encryption. And in the last few years, plenty of other techniques have emerged to trick computers into visiting fake Web sites even without control of the network.

Microsoft says it included the Tunisian government as a trusted certificate authority after it went through the normal application process.

"Microsoft requires that certificate authorities applying to the program provide standardized information," says Bruce Cowper, Microsoft's group manager for trustworthy computing. Tunisia applied in 2006, he said, and its certificate was distributed in February 2007. Venezuela applied in September 2010, and was approved a month later.

Cowper declined to provide information about how many companies, organizations, or governments have failed to pass muster, saying "Microsoft does not share specific information about denied applications, but we do reject applications from certificate authorities who don't meet our criteria (or) fall into one of the named exclusions from the program." Microsoft's [specifications](#) say that any certificate authority that fails an audit, for instance, will be given the boot.

If a certificate authority "isn't in our list it is either because they have not asked to be included, or have not yet been approved," says Opera's Pettersen. "So far, I don't think we have refused any certificate authorities that have applied." Neither Tunisia nor Venezuela have sent Opera an application to be included, he said.

Neither Apple nor Comodo responded to requests for comment.

Comodo Flap Highlights Browser Security Differences

While both Microsoft and [Opera](#) make their criteria public, Mozilla goes further and even makes the [list of pending applications](#) public. Those include a certificate authority operated government of the Valencia region of Spain and Deutscher Sparkassen Verlag GmbH, the world's largest smartcard provider.

As a result of the Comodo breach (Comodo is currently trusted by all the major browsers), there's been talk among Mozilla developers of imposing what amounts to the Internet death penalty: revoking the company's certificate authority, at least until a security audit is performed, from the default Firefox configuration.

Lending ammunition to critics is that this is not the first time that Comodo has experienced a serious security breach. In 2008, a reseller issued an improperly acquired certificate for [Mozilla.org](#).

And Comodo's chief technology officer, Robin Alden, [wrote](#) in February 2010 that, before issuing a certificate, "Comodo performs an automated check of domain control by sending (and confirming receipt of) an email to an address which is either on the domain to be validated or is explicitly mentioned in the Whois entry."

That apparently wasn't done when a Comodo business partner issued those fraudulent certificates earlier this month. Comodo declined to answer questions that CNET posed last week, including the identity of its reseller, what current audits were performed, and how much authority it delegates to partners.

Elinor Mills contributed to this report

The RSA Attack: How They Did It

April 2, 2011, 3:17 PM

The RSA Hack: How They Did It

By [RIVA RICHMOND](#)

The [hack last month](#) at RSA Security has been shrouded in mystery.

How did a hacker manage to infiltrate one of the world's top computer-security companies? And could the data that was stolen be used to impair its SecurID products, which are used by 40 million businesses that are trying to keep their own networks safe from intruders?

The division of [the EMC Corporation](#) is staying mum about what exactly was stolen from its computer systems, aside from that it was data related to SecurID.

But on Friday RSA shed some light on the nature of the attack. In a blog post titled "[Anatomy of an Attack](#)," the company's head of new technologies, Uri Rivner, described a three-stage operation that was similar to several other recent prominent attacks on technology companies, including a 2009 attack on [Google](#) that it said originated in China.

In the attack on RSA, the attacker sent "phishing" e-mails with the subject line "2011 Recruitment Plan" to two small groups of employees over the course of two days. Unfortunately, one was interested enough to retrieve one of these messages from his or her junk mail and open the attached Excel file. The spreadsheet contained malware that used a previously unknown, or "zero-day," flaw in Adobe's Flash software to install a backdoor. RSA said that Adobe had since released a patch to fix that hole.

After installing a stealthy tool that allowed the hacker to control the machine from afar, he stole several account passwords belonging to the employee and used them to gain entry into other systems, where he could gain access to other employees with access to sensitive data, Mr. Rivner said.

Then came stage three: spooling RSA files out of the company to a hacked machine at a

The RSA Attack: How They Did It

hosting provider, and then on to the hacker himself.

The attacker left few traces. But an unclassified document from the United States Computer Emergency Readiness Team (US-CERT) obtained by the blogger [Brian Krebs](#) revealed three Web addresses used in the intrusion, one of which includes the letters “PRC,” which could refer to the People’s Republic of China — or it could be a ruse.

According to Mr. Rivner, it’s difficult for companies with the world’s most sophisticated defenses to stop this newfangled “advanced persistent threats,” which are made potent by the combination of low-tech “social-engineering” cons and a high-tech zero-day attack that antivirus software won’t recognize.

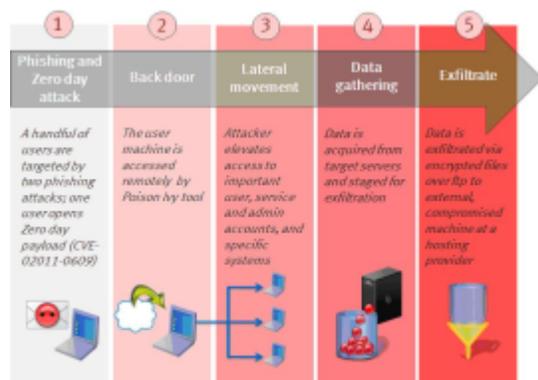
That RSA detected the attack in progress was a victory, he argued. Many other companies hit by similar attacks “either detected the attacks after months, or didn’t detect them at all and learned about it from the government,” he said. “As an industry, we have to act fast and develop a new defense doctrine; the happy days of good old hacking are gone, and gone too are the old defense paradigms.”

But some security experts ridiculed the notion that the attack was sophisticated. Jeremiah Grossman, founder of WhiteHat Security, posted on [Twitter](#): “I can’t tell if this RSA APT blog post is actually being serious or an April 1st gag. The content is absurd either way.”

Attack on RSA Used Zero-Day Flash Exploit in Excel

Attack on RSA used zero-day Flash exploit in Excel

by [Elinor Mills](#)



RSA released this illustration that shows step-by-step how it was attacked.

(Credit: [RSA](#))

The breach at RSA that could compromise the effectiveness of the firm's two-factor authentication SecurID tokens was accomplished via phishing e-mails and an exploit for a previously unpatched Adobe Flash hole, RSA has revealed.

The attacker sent two different phishing e-mails over a two-day period last month with a subject line of "2011 Recruitment Plan" to two small groups of employees who weren't considered particularly high-profile or high-value targets, Uri Rivner, head of new technologies in consumer identity protection at RSA, wrote in a [blog post](#). Attached to the e-mails was an Excel file that contained malware that exploited a hole in Adobe Flash and which installed a backdoor that allowed the attacker to remotely take control of the computer, he wrote.

Adobe [fixed the vulnerability](#) after RSA's announcement, without mentioning that it was used in the RSA attack. (RSA had revealed the breach [last month](#) but did not disclose details on the attack until late last week.)

"The attacker in this case installed a customized remote administration tool known as Poison Ivy RAT (remote administration tool) variant," Rivner wrote. "Often these remote administration tools, the purpose of which is simply to allow external control of the PC or server, are set up in a reverse-connect mode: this means they pull commands from the central command & control servers, then execute the commands, rather than getting commands remotely. This connectivity method makes them more difficult to detect, as the PC reaches out to the command and control rather than the other way around."

The type of attack RSA was hit with is known as an "Advanced Persistent Threat" (APT). Such attacks are often used to target source code and other information useful in espionage, and they involve knowledge of the company's operations, network, and employees and their roles. With APTs, attackers often have months to snoop around the network and gather information. But RSA

Attack on RSA Used Zero-Day Flash Exploit in Excel

stopped this attack early on, although the attacker still had time to "identify and gain access to more strategic users," Rivner said. "Since RSA detected this attack in progress, it is likely the attacker had to move very quickly to accomplish anything in this phase," he added.

"The attacker first harvested access credentials from the compromised users (user, domain admin, and service accounts). They performed privilege escalation on non-administrative users in the targeted systems, and then moved on to gain access to key high value targets, which included process experts and IT and Non-IT specific server administrators," he said.

The RSA attacker then copied targeted data and moved it to servers inside the company where it was aggregated, compressed, and encrypted and then sent to a server at a hosting provider that had been compromised, according to Rivner. The File Transfer Protocol (FTP) was used to transfer "many" password-protected RAR (Roshal Archive) files from the RSA file server to the outside server before they were removed to remove any traces of the attack, according to Rivner.

As interesting as the blog post is on how the attack was accomplished, it leaves out the most important information about the attack: what data was stolen. This is the key information that SecurID customers need to assess their risk and decide what to do to protect their networks.

Initially, [experts speculated](#) that a database containing unique numbers for each token was stolen, but that information would still need to be combined with a secret key, called a "seed," to generate the one-time passcodes that flash on the tokens. An attacker would have to somehow predict the seed, as well as know the password associated with the user. RSA has been mum about this information which could hint at its secret sauce.

Chris Wysopal, chief technology officer at application security firm [Veracode](#), said several information security professionals he has talked to whose companies use SecurID were told by RSA that there is an algorithm that maps the serial number of the token to the seed and that that algorithm was stolen by the attackers. "The risk here is any way the attackers can get access to a serial number they can get access to the seed," Wysopal said in an e-mail. "The serial numbers used by an organization might not be well protected."

In a follow up telephone interview with CNET today, Wysopal said he has not been able to verify that information with RSA. "But it makes sense to me. If it's a design weakness they wouldn't want to talk about it," he said. "We haven't been able to confirm it, but as an RSA customer ourselves it's something we are bringing into our threat model" for figuring out how to best secure the network.

An RSA spokesman declined to comment beyond what the company has said in its public announcements and blog posts. RSA has also released this [post](#) in which Mischel Kwon, RSA consultant and former deputy director for IT Security Staff at the U.S. Department of Justice, commends the company on how it has responded to the incident and notified customers.

RSA has sent security advisory notes to 60,000 customers, briefed 15,000 customers, and had one-on-one briefings with hundreds of customers in sensitive industries who have signed non-

Attack on RSA Used Zero-Day Flash Exploit in Excel

disclosure agreements to talk more specifically about how they can best protect themselves, a source close to RSA told CNET.

An Attack Sheds Light on Internet Security Holes

An Attack Sheds Light on Internet Security Holes

By RIVA RICHMOND

Published: April 6, 2011

The Comodo Group, an Internet security company, has been attacked in the last month by a talkative and professed patriotic Iranian hacker who infiltrated several of the company's partners and used them to threaten the security of myriad big-name Web sites.

But the case is a problem for not only Comodo, which initially believed the attack was the [work of the Iranian government](#). It has also cast a spotlight on the global system that supposedly secures communications and commerce on the Web.

The encryption used by many Web sites to prevent eavesdropping on their interactions with visitors is not very secure. This technology is in use when Web addresses start with "https" (in which "s" stands for secure) and a closed lock icon appears on Web browsers. These sites rely on third-party organizations, like Comodo, to provide "certificates" that guarantee sites' authenticity to Web browsers.

But many security experts say the problems start with the proliferation of organizations permitted to issue certificates. Browser makers like [Microsoft](#), [Mozilla](#), [Google](#) and [Apple](#) have authorized a large and growing number of entities around the world — both private companies and government bodies — to create them. Many private "certificate authorities" have, in turn, worked with resellers and deputized other unknown companies to issue certificates in a "chain of trust" that now involves many hundreds of players, any of which may in fact be a weak link.

The Electronic Frontier Foundation, an online civil liberties group, has explored the Internet in an attempt to [map this nebulous system](#). As of December, 676 organizations

An Attack Sheds Light on Internet Security Holes

were signing certificates, it found. Other security experts suspect that the scan missed many and that the number is much higher.

Making matters worse, entities that issue certificates, though required to seek authorization from site owners, can technically issue certificates for any Web site. This means that governments that [control certificate authorities](#) and hackers who break into their systems can issue certificates [for any site at will](#).

Experts say that both the certificate system and the technology it employs have long been in need of an overhaul, but that the technology industry has not been able to muster the will to do it. “It hasn’t been perceived to be a big enough problem that needs to be fixed,” said Stephen Schultze, associate director of the [Center for Information Technology Policy](#) at Princeton. “This is a wake-up call. This is a small leak that is evidence of a much more fundamental structural problem.”

In the Comodo case, the hacker infiltrated an Italian computer reseller and used its access to Comodo’s systems to automatically create certificates for Web sites operated by Google, [Yahoo](#), Microsoft, [Skype](#) and Mozilla. With the certificates, the hacker could set up servers that appear to work for those sites and try to view the unscrambled e-mail of millions of people, experts say.

In a series of online messages teeming with bravado, the hacker described himself as a software-engineering student and cryptography expert and said he worked alone. He suggested he was avenging the [Stuxnet](#) computer worm, which was directed at Iranian nuclear installations last year. And he indicated that he intended to use the certificates he created to snoop on opponents of the Iranian regime. “As I live, you don’t have privacy in Internet, you don’t have security in digital world,” he warned.

Comodo’s chief executive, Melih Abdulhayoglu, said that “the system we have has been

An Attack Sheds Light on Internet Security Holes

serving us well,” though it could be improved. His firm’s processes were adequate based on the known threats, but have now been tightened, he said.

The certificate system was created at the dawn of e-commerce in the early 1990s before security was a major issue. Security experts say the system is not up to the challenge of today’s immense, commercial and much-attacked Internet. It was designed primarily to let businesses take credit card payments online, and less to confirm the authenticity of Web sites.

The crucial tool available to Comodo and the browser makers — revocation — is ineffective, security experts say. After the Comodo case, Google, Mozilla and Microsoft rushed out patches so their browsers would recognize and reject the bad certificates. But this solution requires many millions of Internet users to update their browser software, which many people never do.

Moreover, because certificate authorities’ servers are seen as unreliable, most browser makers allow users to proceed to an alternative site, and hackers can exploit this weakness, security experts say.

Browser makers have another problem: Faced with a suspicious certificate authority, there is little they can do shy of rescinding it. But if they did that, millions of Web users might encounter troubling error warnings when they visited sites with certificates from that company, causing a cascade of problems for users and site owners. Cutting out a large player like Comodo, which controls at least 95,100 certificates, could effectively “break the Web,” said Dan Kaminsky, chief scientist at the security firm DKH.

They are effectively “too big to fail,” said Christopher Soghoian, a former Federal Trade Commission technologist who is now a graduate fellow at the [Center for Applied Cybersecurity Research](#) at [Indiana University](#). “The problem is that the browser vendors

An Attack Sheds Light on Internet Security Holes

don't have a small stick, they only have a big stick."

Microsoft and Mozilla said that they would consider removing certificate authority if it was in the best interest of Internet users, and that they remained in talks with Comodo about its security practices. "Participation in Mozilla's root program is a privilege, not a right," the company, the nonprofit maker of Firefox, said. Apple, maker of the Safari browser, declined to comment. (Google's Chrome browser defers to the choices of operating system makers like Microsoft and Apple about which certificate authorities are accepted.)

Mozilla, Microsoft and Google said they would work together and with certificate authorities and the security community on improvements to the system. [One approach](#) proposed by Comodo and Google engineers in January would allow Web site owners to specify which certificate authorities may issue certificates for their sites.

[An initiative](#) preferred by security experts would overhaul the system more radically. It would give Web sites similar control while securing their certificates within a new encrypted version of the domain name system, the central directory of the Web, making it the de facto central certificate authority through which Web sites could generate their own certificates.

NASA Network Holes May Jeopardize Missions

March 29, 2011 5:04 PM PDT

[NASA network holes may jeopardize missions](#)

by [Elinor Mills](#)

Weak security practices and critical holes in NASA's agency-wide network could allow an attack over the Internet that would disrupt missions and expose sensitive data, according to a government report.

"Until NASA addresses these critical deficiencies and improves its IT security practices, the Agency is vulnerable to computer incidents that could have a severe to catastrophic effect on Agency assets, operations, and personnel," said the Inspector General's report, titled "[Inadequate Security Practices Expose Key NASA Network to Cyber Attack \(PDF\)](#)," released yesterday.

NASA uses a series of networks to carry out its various missions, which include controlling spacecraft like the International Space Station and conducting science missions like the Hubble Telescope.

The Office of Inspector General (OIG) found that servers on the NASA network had "high-risk" vulnerabilities that were exploitable from the Internet and that specifically six servers containing critical data and used for controlling spacecraft were found to have holes that would allow a remote attacker to take control over them or render them inaccessible. Once inside the network, an attacker could exploit other weaknesses auditors identified, which could "severely degrade or cripple NASA's operations," the report said.

Poorly configured network servers revealed encryption keys and encrypted passwords and one server disclosed sensitive account data for all its authorized users. The information could be used to target NASA personnel with phishing attacks and e-mails containing malicious code designed to compromise the recipient's computer.

The OIG recommended last May that NASA immediately establish an IT (information technology) security oversight program for the key network. As of last month, such a program was not implemented despite the fact that NASA agreed with the recommendation, the report said.

The problems are not just theoretical; NASA's network has been breached. In January 2009, attackers stole 22 gigabytes of export-restricted data from a Jet Propulsion Laboratory computer system, according to the report. Later that year, a computer system that supports one of NASA's mission networks was infected and was causing the system to make more than 3,000 unauthorized connections to domestic and international Internet Protocol addresses including addresses in China, the Netherlands, Saudi Arabia and Estonia, the OIG said.

"The sophistication of both of these Internet-based intrusions confirms that they were focused and sustained efforts to target assets on NASA's mission computer networks," the report said.

NASA representatives could not be reached for comment late today.

NASA Network Holes May Jeopardize Missions

Microsoft Wins a Botnet Battle

Microsoft Wins A Botnet Battle

Posted by Dave Methvin on Tuesday Mar 29th at 7:00am

If you noticed a decrease in spam recently, there could be a good reason. This month, Microsoft [took down](#) the Rustok botnet.

Microsoft's Digital Crime Unit reported that its "research shows there may be close to one million computers infected with Rustock malware, all under the control of the person or people operating the network like a remote army, usually without the computer's owner even aware that his computer has been hijacked. Bot-herders infect computers with malware in a number of ways, such as when a computer owner visits a Web site booby-trapped with malware and clicks on a malicious advertisement or opens an infected e-mail attachment. Bot-herders do this so discretely that owners often never suspect their PC is living a double life."

These botnets aren't just the toy of young hackers who like causing mischief. They aren't trying to crash or disable the computer; in fact it's just the opposite. That stealth aspect to the bot infection is key to its success. The user has no reason to think they need to get their PC fixed, because a good botnet infection doesn't raise suspicion. That is the key to the botnet's survival.

A botnet is a huge money-making tool for its creators. When bot-herders take over a PC, they have many ways to turn a profit. One way is to grab information they find on the PC, or can extract by monitoring the user's keystrokes. This can give them access to bank accounts, credit cards, and login information to sites such as eBay or PayPal. Before the user can do anything to stop it, the botnet operator can transfer the PayPal money to another account. Or they can purchase expensive items with the user's eBay account and get the seller to send it to an address where the botnet operator can pick it up.

Perhaps the most valuable thing a botnet provides its handler is a large pool of "innocent-looking" IP addresses. In the case of the Rustok botnet, that's one million IPs. If the bot-controlled PC appears to visit a Web site, click on a Google Adwords ad, or send a few dozen emails, it's not possible to block that action based merely on the IP address. So Rustok's botnet could send 10 million spam messages by having each PC send just 10 emails, and nothing looks suspicious.

Click fraud is another endless source of money for botnet operators. By setting up some shallow content sites with Google Adwords or other ad networks, the bot-herder can have the bots visit those sites and click on the ads to generate revenue. The bot-herder can also use click fraud to attack competitors, clicking on their ads in order to drain their ad budgets. This type of fraud can be extremely difficult for the ad networks

Microsoft Wins a Botnet Battle

to spot if the botnet operator keeps the fraud at a low level and doesn't get too greedy. When botnets started to emerge a decade ago, the creators of the botnet often used them directly and managed all the money-making schemes themselves. Now, many bot-herders rent out their botnet to other groups that have specific goals in mind, such as spam, click fraud, or targeted attacks. Underground message boards let bot-herders communicate with their customers to "sell time" on the botnet. Botnets are a threat not only to businesses and consumers, but to governments as well. A botnet can be used as a huge army in [cyberwarfare](#), effectively disabling communication channels by clogging critical Internet paths or Web sites. Unlike many weapons programs, a botnet can be self-funding and doesn't require technology that's embargoed by major nations like the United States. The commercial crime not only brings in money, but provides a "cover story" for why the botnet was created in the first place. At any point, however, the botnet can become a weapon of war if it is controlled by a country.

Microsoft has its own take on how to combat botnets: "It's like a gang setting up a drug den in someone's home while they're on vacation and coming back to do so every time the owner leaves the house, without the owner ever knowing anything is happening. Homeowners can better protect themselves with good locks on their doors and security systems for their homes. Similarly, computer owners can be better protected from malware if they run up-to-date software -- including up-to-date antivirus and antimalware software -- on their computers.

Although antimalware software can help, its effectiveness is far from perfect. The botnet creators are constantly working on ways to mask their infection vectors, and are often successful. Combine that with the gullibility of many users and some simple social engineering techniques ("free porn, don't worry about the antivirus warning, it's a known bug") and many PCs that are technically protected still become infected. Once it's established on the PC, the botnet software often disables any antivirus software, and may even turn off Windows Updates to prevent programs like the Microsoft Malicious Software Removal Tool from running.

Large enterprises can be a prime source of raw PC material for botnets, but they also have tools that consumers don't have for detecting and fixing botnet infections. The most important of these are network monitoring. Botnets have to communicate with a "controller" on the Internet in order to receive their marching orders. By analyzing the Internet traffic traveling through the corporate firewall, the network admins may be able to find suspicious patterns.

Botnet operators are often opportunistic in their attacks. If they happen to find that they have taken over a PC in an enterprise, they may sell the control of that PC to someone who would like to make a targeted attack on that company. At that point it's no longer just a case of your company's PCs being used for bad things. Your company's PCs have become a vector being used to attack the company itself. The potential for losses

Microsoft Wins a Botnet Battle

of both money and information are almost unlimited. That risk alone is the best justification for your company to actively monitor and combat its PCs being turned into botnet fodder.

Social-media Tools Used to Target Corporate Secrets

Social-media tools used to target corporate secrets

By [Byron Acohido](#), USA TODAY

Not long after airstrikes began in [Libya](#) earlier this month, certain attorneys at four U.S. law firms, known for having high-profile clients in the oil industry, each received a personally addressed e-mail message.

Each message carried an Adobe PDF attachment, purportedly an analyst report describing the impact of Libya's uprising on oil futures. Each lawyer clicked on the attachment.

But the PDF was actually pre-set to deliver a quick-acting computer intrusion, says Chris Day, chief security architect at data security firm Terremark, who watched the attack unfold. Within a few seconds, the PC of each attorney who clicked on the attachment began sending a silent beacon to a command server controlled by the intruders.

Terremark alerted law enforcement, and the law firms were notified, cutting off yet another persistent intrusion — a distinctive type of hack that has quietly become a staple of the cyberunderground.

“We’re seeing criminal gangs using these tactics against commercial enterprises simply because they work so well,” says Day.

Such so-called spear-phishing attacks, which often enlist social-media tools to meticulously wedge into corporate networks, are increasingly used in computer thefts that pinpoint valuable corporate data, according to a report released today by IBM's X-Force cybersecurity team.

“Cybercriminals have become more focused on quality of attacks, rather than quantity,” says [Tom Cross](#), X-Force threat intelligence manager.

Elite cybercriminals are tapping into search engines and social networks

Social-media Tools Used to Target Corporate Secrets

to help them target specific employees for social-engineering trickery at a wide range of companies, professional firms and government agencies. They wait patiently for an opportune moment to seed an infection, knowing they need only infect one well-placed PC to gain a foothold inside a company network. They then proceed to stealthily probe deeper over many months.

“It’s become very common for advanced groups to be in systems for a year or longer without being detected,” says Kim Peretti, forensics director at [PricewaterhouseCoopers](#).

The booty of choice: intellectual property.

Proprietary intellectual property is generally considered twice as valuable as day-to-day financial and customer data, according to [Forrester Research](#). A thriving criminal market has evolved for converting stolen trade secrets into cash, say security experts and law enforcement officials. Demand is being driven by Asian companies looking to undercut Western rivals, and by scam artists seeking to game stocks and commodities markets. Persistent intrusions keep stolen company secrets flowing into this underground market.

Cybercriminals have “shifted their focus to trade secrets and product planning documents,” says Simon Hunt, chief technology officer of [McAfee](#)’s Endpoint Security division.

Rampant attacks

Yet, only a minority of persistent intrusions are being detected, and fewer still are disclosed publicly, as companies are loath to announce that they’ve been breached. McAfee estimates that just three in 10 organizations report all data breaches.

Social-media Tools Used to Target Corporate Secrets

Even so, a spate of high-visibility hacks that have recently come to light gives a glimpse at the scale and profitability of persistent intrusions.

Earlier this year, companies participating in Europe's carbon registries lost some \$50 million to an Eastern European gang that infiltrated their trading systems. Nasdaq last month admitted that intruders roamed undetected for at least a year deep inside its cloud-based collaboration service, called Director's Desk, whose users are senior executives and board members of big public companies.

In a typical month, threat-detection company Mandiant is busy investigating some 30 to 40 persistent intrusions in organizations around the world. It's just one of several security firms that specialize in such investigations.

"There have been thousands of compromised organizations in the United States alone over the last five years," says Kevin Mandia, CEO of Mandiant. "In the last 18 months, we've responded to approximately 100 different organizations in North America and throughout the world who were hacked by criminals operating out of Asia."

Criminal gangs in China, Russia and Ukraine, in particular, appear to be in the vanguard of such attacks, Mandia says. They've quickly and astutely moved to take full advantage of the corporate sector's embrace of Internet-based technologies.

Social-media weapons

For instance, many attacks Mandiant has investigated began with the criminals doing reconnaissance on [Google](#), [Facebook](#), [LinkedIn](#), [Twitter](#) and other popular Internet services to find companies to target — and pinpoint specific executives, researchers, analysts, engineers or key

Social-media Tools Used to Target Corporate Secrets

administrative assistants to attack.

The next step is to craft a spear-phishing lure designed to entice a specific employee to click on a viral attachment or Web page link, using information gleaned during the reconnaissance phase to make the attachment or link seem trustworthy. In 2010, criminals increasingly used e-mail, instant messages and social-network posts to spear phish targeted employees, says IBM's Cross.

One enterprising gang recently put a twist into spear phishing by noticing that more than a few executives have a penchant for using Google Alert in connection with their names. Google's free service will e-mail a Web link to the executive every time the search engine indexes a Web page containing a fresh news article mentioning the executive.

The intruders figured out how to inject an infection onto such Web pages at just the right moment, so the infection has a low chance of being detected and a high chance of appearing as part of a Google Alert arriving in the executive's in-box, says Mickey Boodaei, CEO of security firm Trusteer.

One way they do this is by putting up an infectious Web page that redirects to a legitimate Web page carrying a news article about the executive; the link between the bad and good sites is enabled just after Google indexing has occurred. "These targeted attacks are very powerful and should be taken very seriously," Boodaei says.

Once an initial infection takes hold, persistent intruders seek to gain wider and deeper access to an organization's network. This typically means pilfering a system administrator's user name and password to gain escalated privileges; there are myriad proven techniques for accomplishing this.

With escalated privileges, the intruders can map the layout of the network

Social-media Tools Used to Target Corporate Secrets

and make note of key servers that control e-mail and store data. They also routinely disable antivirus protection and install “multiple backdoors with different configurations,” setting up options for re-infecting the network should they be detected, says Mandia.

In one case, a company discovered 100 infected computers, took them off line, and hired Mandiant to confirm its network was clean. Investigators found the intruders used backdoors to freshly infect 20 workstations and servers. By quickly removing the 100 infected PCs, the company alerted the intruders, who changed tactics. “The problem with immediately removing compromised systems is that it typically alerts the attacker and lets them know an infected system has been identified,” says Mandia.

Another pitfall for companies is not knowing what’s been stolen. Borrowing techniques developed in the cyberespionage world, persistent intruders can easily hide their tracks.

Few details have been disclosed about the Nasdaq breach last month, other than that “suspicious files” were found lurking for an extended period on a server supporting Directors Desk. Think of Directors Desk as a no-nonsense social network for very privileged users. Nasdaq describes it as a “complete turn-key, fully-hosted online board (of directors) technology solution, with over 5,000 users representing more than 175 organizations worldwide, including many *Fortune* 500 companies.”

Corporate treasures

Nasdaq quickly issued a statement saying “there is no evidence that any Directors Desk customer information was accessed or acquired by hackers.”

Nicholas Percoco, who heads SpiderLabs at data security firm Trustwave,

Social-media Tools Used to Target Corporate Secrets

and Uri Rivner, head of new technologies, identity protection and verification at RSA, security division of EMC, say it seems most plausible that whoever inserted the suspicious files used a classic persistent-intrusion attack.

“Whoever did this was definitely targeting the Holy Grail of insider information,” Rivner says. “In the past year, we’ve seen more and more evidence of cybercriminals targeting specific individuals in private-sector corporations.”

Percoco says the intruders were “probably going after very valuable, company-confidential information, such as financial results prior to their being announced, mergers and acquisitions under consideration, company plans, product roadmaps, IPOs, all those types of things that would be available to members of a board.”

The quickest route to profits would be for the intruders to harvest insider information, then make trades to game the stock market. But it could take months or years for cyberforensics and market experts to ferret out evidence.

McAfee and Science Applications International recently surveyed 1,000 senior information technology professionals in the U.S., [United Kingdom](#), Japan, China, India, Brazil and the Middle East. Some 25% of organizations participating reported they had a merger, acquisition or product roll-out “stopped or slowed by a data breach or the credible threat of a data breach.” And 62% of respondents expressed concern that securing company secrets is going to get more problematic with the rising use of Internet-connected smartphones, tablet PCs and e-readers in workplaces.

“Criminals are attacking corporate intellectual capital, and they are often

Social-media Tools Used to Target Corporate Secrets

succeeding,” says McAfee’s Hunt.

DHS Seeks to Grow Antibodies in Cyberspace

DHS seeks to grow antibodies in cyberspace

March 27, 2011 — 7:58pm ET | By [David Perera](#)

A white paper released March 23 by the Homeland Security Department says a tripartite approach to cybersecurity based on automation, interoperability and authentication could make networks fundamentally more secure.

The paper envisions a future in which networked devices communicate in near real-time about attacks and react in a coordinated manner based on a policy framework. Some simulations of such a cybersecurity model, the white paper says, indicate that only 30 to 35 percent of devices would need to cooperate in order to defeat an attack, meaning that a large-scale modification of existing infrastructure wouldn't be necessary for implementation.

The paper draws heavily on an immune-system analogy, positing that cybersecurity should become a matter of "automated courses of action" in which devices sense malicious actors and enact defensive responses on their own.

The first building block in making that possible, automation, would require devices endowed "with strong feed forward and feedback signaling mechanisms" that can accommodate communication failures.

Authentication would allow devices a heightened ability to observe, record and share data, the paper adds. An authentication mechanism would have to "recognize that trust is not a binary or static state, but is fluid and conditioned upon evolving operations and environmental factors." Authentication would extend beyond persons to include computers, software and information itself.

Of the three elements in the tripartite approach, the paper spends the most time on interoperability, which itself has three types--semantic, technical and policy. Semantic is the ability of parties to understand a message in the sense intended by the sending party, technical the practical ability to send the messages, and policy is common business processes related to the transmission, receipt and acceptance of data.

The paper also suggests a maturity model for assessing how much various communities adopt the immune system model, adding that the scale isn't normative, since some communities could opt to operate at lower levels for reasons of cost or efficiency.

DHS Seeks to Grow Antibodies in Cyberspace

Creating the model will require a government role, the paper heavily suggests.

"Adoption of security standards is decidedly slow, and early indications are that cybersecurity continuous monitoring will face impediments to adoption. This indicates an imbalance of incentives, whereby defenders are not incented, but attackers are," the paper states, echoing a [common refrain](#) among [federal officials](#) who have been making a public argument for a stronger government role in the cybersecurity of private sector critical infrastructure.

One way to set up a greater government role would be to create a "Cyber Center for Disease Control and Prevention," the paper states. A Cyber CDC would watch for threats and incidents, disseminate data, perform threat analysis, make recommendations and coordinate preventive actions, the paper adds.

The paper says that governance questions are not easily suggested, however, acknowledging that questions of liability (either for deploying countermeasures, or for failing to deploy them), who would have the power to compel action and to set policy as well as the role of state, national and international entities are all unanswered.

The paper solicits comments, sent to cyberfeedback@dhs.gov, and promises a follow-up paper that incorporates public observations and that "at a minimum, identifies key game-changing initiatives for each of the three building blocks."

The Asymmetrical Online War

April 3, 2011, 6:48 AM

The Asymmetrical Online War

By [JOHN MARKOFF](#)

In 1975, John Brunner wrote a science fiction novel, “The Shockwave Rider,” about a lone programmer who creates a computer worm that exposes a repressive regime’s secrets and ultimately undermines a tyrannical government.

Life invariably seems to find a way to imitate art, but as the world’s computer systems and networks continue to fall prey to hackers, the resemblance has become eerie. The Internet has transformed many things in the world, but one of its most remarkable effects has been to change the balance of power, not between states, but between entire nations and their citizens.

“It’s a completely surreal realization that nation states can be seriously confronted by teenagers, but that’s where we’re at,” said John Perry Barlow, the [Grateful Dead](#) lyricist who co-founded the Electronic Frontier Foundation in 1990 to help defend young computer hackers. “One very smart person can take on an entire nation state.”

One can take on the security apparatus of the Web as well. In the space of a little more than a month, two computer security firms have been publicly humiliated, one by an anonymous computer hacker who claimed in an e-mail interview with a Forbes columnist to be a 16-year-old girl and a second by someone who is apparently a 21-year-old Iranian who later appeared online as a proponent of [Mahmoud Ahmadinejad](#)’s government to rail against the West.

Also last month, RSA, a Massachusetts-based firm that sells software to corporations and governments that is used to keep digital secrets, was forced to admit that it had been the victim of what the firm described as a mysterious “Advanced Persistent Threat,” potentially undermining crucial encryption technology that protects millions of computers around the globe.

The Asymmetrical Online War

Each incident underscored the potential power of an individual or a small group in cyberspace — from destroying a company’s reputation to fundamentally undermining the digital security of millions of Internet users.

“There is asymmetry in resources, in time, in response, in cycle time, in information sharing, and maybe even in other areas as well, depending on the kind of attack and attackers,” said Eugene Spafford, a computer scientist and computer security specialist at [Purdue University](#).

Not long ago all this might have been the stuff of science fiction, but the dystopian world that was envisioned by Mr. Brunner, as well as similar future political scenarios drawn by a generation of “cyberpunk” science fiction writers like [Neal Stephenson](#), William Gibson and Vernor Vinge, seem increasingly to be echoed by real world events.

Indeed, it is not a coincidence that the political sensibilities of the [Wikileaks](#) founder [Julian Assange](#) were shaped by his participation in the Cypherpunk digital anarchist movement of the 1990s, which in turn drew inspiration from novels of cyberpunk science fiction authors like Mr. Gibson and Mr. Stephenson.

Hardly a week passes when there isn’t some new incident underscoring the fundamental imbalance of power in cyberspace between attacker and defender, where a highly motivated and reasonably skilled intruder, operating in secrecy from almost anywhere in the world, can with apparent ease unravel digital fortifications intended to offer banking-grade security.

In February, an executive at HBGary, a Sacramento, Calif., security software and consulting firm, made the mistake of publicly boasting that he had unmasked the identities of the members of [Anonymous](#), a secretive collection of cyber-vigilantes who had attracted attention by launching Internet denial-of-service attacks in defense of Wikileaks. The security company, which was engaged in a series dubious business

The Asymmetrical Online War

propositions, soon found that the details of its business were exposed to the world. Anonymous, whose ringleader was possibly a teenager, tricked one of the company's systems administrators into giving them password information, making it possible to steal more than 50,000 of HBGary's e-mail messages and placing them on a Russian web site.

Last month, Comodo, a Jersey City, N.J., supplier of computer security products, including certificates used for authenticating digital identity online, said that it had suffered an elaborate electronic break-in and theft by someone who appeared intent on using stolen certificates to compromise the e-mail and social network accounts of Iranian dissidents. Suspicions first focused on a group of patriotic Iranian hackers known as the Iranian Cyber Army, but within days a young Iranian computer hacker convincingly claimed credit for the exploit. Modesty was not one of his character traits: "I know you are really shocked about my knowledge, my skill, my speed, my expertise and entire attack. That's O.K., all of it was so easy for me," he wrote in a post. He also vaguely hinted that the theft was revenge for the [Stuxnet](#) computer worm, which may have been unleashed last year by Israel and the United States in an effort to undermine Iran's nuclear weapons efforts.

The RSA compromise last month sent new shockwaves through corporate boardrooms and banking headquarters, as well as dozens of the nation's defense contractors. The implications were that somewhere there was a brilliant black hat hacker who was only a step away from being able to electronically waltz into the best-protected American networks.

For his part, Mr. Barlow said he remained an optimist about the Internet's effect on the balance of power.

"It really depends on your view of human nature," he said.

US Shuttters Botnet, Can Disable Malware Remotely

U.S. shuts botnet, can disable malware remotely
by Elinor Mills

By seizing servers and domain names and getting permission to remotely turn off malware on compromised PCs, U.S. officials have disabled a botnet that steals data from infected computers.

The legal actions are part of the "most complete and comprehensive enforcement action ever taken by U.S. authorities to disable an international botnet," according to a [statement](#) from the Department of Justice. A botnet is a group of computers that have been compromised and are being remotely controlled by attackers, typically to send spam or attack other computers.

It's the first time law enforcement in the U.S. has requested permission from a court to take control of a botnet, according to a [request for a temporary restraining order](#) that was granted. Similar action was taken by Dutch officials who downloaded "good" software to computers infected with Bredolab botnet malware, the filing said.

In this case the malware, called "Coreflood," records keystrokes and private communications, enabling it to steal usernames, passwords, and other private personal and financial information. Once a computer is infected with Coreflood, the malware communicates with a command-and-control server, allowing it to remotely control the compromised computer. The botnet is believed to have infected more than 2 million Windows-based computers worldwide in nearly 10 years.

Prosecutors allege that data stolen by the malware has been used to steal funds from victims' accounts. In at least one case, the malware enabled attackers to take over an online banking session a victim was in the middle of and transfer money to a foreign account, according to court filings.

The U.S. Attorney's office in the district of Connecticut has filed a civil complaint against 13 "John Doe," or unknown, defendants accusing them of wire fraud, bank fraud, and illegal interception of electronic communications. To shut down the botnet and stop it from spreading further, the Justice Department seized five command-and-control servers and 29 domain names used by the bots to communicate with the servers.

To put a halt to the botnet's damage to already infected computers, officials have obtained a temporary restraining order authorizing them to substitute the seized servers with their own and use them to respond to signals sent from hundreds of thousands of compromised computers in the U.S. This will allow authorities to send commands to the infected computers that stop the malware from running, preventing attackers from updating the malware and giving victimized computers time to update their virus signatures.

Officials also are working with Internet Service Providers to identify owners of the compromised computers based on their IP addresses and warn them about the potential for fraud because of the malware on the machines. Computer owners will be told how to "opt out" if they do not want officials to stop the malware from running on their machines. "At no time will law enforcement

US Shuttters Botnet, Can Disable Malware Remotely

authorities access any information that may be stored on an infected computer," the statement said.

"Allowing Coreflood to continue running on the infected computers will cause a continuing and substantial injury to the owners and users of the infected computers, exposing them to a loss of privacy and an increased risk of further computer intrusions," Judge Vanessa Bryant wrote in her decision granting the temporary restraining order.

The substitute command-and-control server will be operated by the nonprofit Internet Systems Consortium under law enforcement supervision, according to court documents. Microsoft, meanwhile, was expected to update its Malicious Software Removal Tool yesterday to remove Coreflood from infected computers, the filing dated yesterday says.

While the actions have disabled Coreflood in its current form, other variants of the malware could still be lurking on the Internet, officials said.

From March 2009 through January 2010, one Coreflood server had about 190 gigabytes of data from 413,710 infected computers, the court filing shows. Of known victims, a real estate company in Michigan was defrauded out of \$115,771; a law firm in South Carolina lost \$78,421, an investment company in North Carolina lost \$151,201; and a defense contractor in Tennessee lost \$934,528, the document says.

The Justice Department is working with the FBI, the U.S. Marshals Service, and the U.S. Attorney's office in Connecticut with help from Microsoft and the Internet Systems Consortium.

Malware Writers Making Code Tougher to Decode, Harder to Find

Malware Writers Making Code Tougher To Decode, Harder To Find

Malicious code is more frequently scrambled, encrypted to foil would-be reverse engineers

Apr 13, 2011 | 05:29 PM | [1 Comments](#)

By Robert Lemos, Contributing Writer

Darkreading

Decoding the methods in malicious code is becoming more difficult, according to reverse-engineering experts. Attacks no longer scramble simple function names, but encrypt entire blocks of code.

Attackers use obfuscation to make it harder to analyze malicious software and stymie security tools, such as intrusion-detection systems, from recognizing the attack. Initially, obfuscation merely scrambled the names of the functions being called by a program, complicating analysis of the binary code.

As automated reverse engineering makes progress, however, malware authors are increasingly scrambling entire blocks of code and using better obfuscation techniques to make analysis and detection that much harder, says Adam Meyers, director of cybersecurity operations for SRA International. "At the business end of the malware, it is getting very complex and confusing," says Adam Meyers, director of cybersecurity operations for SRA International. Meyers will speak at the [SOURCE Boston conference](#) next week in a talk on reverse-engineering techniques to deal with obfuscation.

Part of the problem is that attackers are using so many different ways of getting onto systems, experts say. Attacks that use social engineering will use obfuscated Web addresses and code. Drive-by downloads, which infect people when they visit a website, will encrypt their payloads. And more direct measures aimed at servers will scramble the code to evade intrusion-detection systems, says Matt McKinley, director of product management at network security firm Stonesoft.

"The battle from the defenders' side is big," McKinley says. "There is a lot of things that you have to reverse engineer."

Reverse engineering has become an extremely important security function. In March, online giant Google bought reverse-engineering firm Zynamics, the maker of a number of tools to help analyze binary executables.

Malware Writers Making Code Tougher to Decode, Harder to Find

Currently, most obfuscation is simple, using operations such as XOR-ing bits or rotating through alphanumeric characters, says SRA's Meyers, who spent three years at the U.S. State Department handling security and reverse-engineering attacks. Increasingly, however, the attackers are using better encryption or customized functions to make reverse engineering more difficult.

Oddly, the targeted attacks that most call "advanced persistent threats" (APTs) are not always the most difficult to reverse engineer, Meyers says. The mercenary developers that create software for cybercriminals are more likely to use encryption and other advanced forms of obfuscation. One reason is that competition in the malware market has led to better tools. In addition, commercial malware increasingly uses digital rights management (DRM) technology to prevent customers from becoming competitors.

"I've seen people say things about APT -- targeted attacks -- who may not have been familiar with APT," Meyers says.

The newer the malware category, the more likely that better obfuscation will be used, experts say. Meyers, for example, has encountered DES encryption obfuscating mobile malware. DES stands for data encryption standard, an older method for scrambling data that is no longer considered secure but is more than adequate for obfuscation.

"People that are writing new malware are fixing a lot of the mistakes that had been made before," Meyers says.

US Shuts Down Massive Cyber Theft Ring

U.S. shuts down massive cyber theft ring

Wed Apr 13, 2011 6:55pm EDT

By Diane Bartz and Jim Finkle

WASHINGTON/BOSTON (Reuters) - U.S. authorities claimed one of their biggest victories against cyber crime as they shut down a ring they said used malicious software to take control of more than 2 million PCs around the world, and may have led to theft of more than \$100 million.

A computer virus, dubbed Coreflood, infected more than 2 million PCs, enslaving them into a "botnet" that grabbed banking credentials and other sensitive data its masters used to steal funds via fraudulent banking and wire transactions, the U.S. Department of Justice said on Wednesday.

The government shuttered that botnet, which had operated for a decade, by seizing hard drives used to run it after a federal court in Connecticut gave the go-ahead.

"This was big money stolen on a large scale by foreign criminals. The FBI wanted to stop it and they did an incredibly good job at it," said Alan Paller, director of research at the SAN Institute, a nonprofit group that helps fight cyber crime.

The vast majority of the infected machines were in the United States, but the criminal gang was likely overseas.

"We're pretty sure a Russian crime group was behind it," said Paller.

Paller and other security experts said it was hard to know how much money the gang stole. It could easily be tens of millions of dollars and could go above \$100 million, said Dave Marcus, McAfee Labs research and communications director.

A civil complaint against 13 unnamed foreign nationals was also filed by the

US Shuts Down Massive Cyber Theft Ring

U.S. district attorney in Connecticut. It accused them of wire and bank fraud. The Justice Department said it had an ongoing criminal investigation.

The malicious Coreflood software was used to infect computers with keylogging software that stole user names, passwords, financial data and other information, the Justice Department said.

"The seizure of the Coreflood servers and Internet domain names is expected to prevent criminals from using Coreflood or computers infected by Coreflood for their nefarious purposes," U.S. Attorney David Fein said in a statement.

In March, law enforcement raids on servers used by a Rustock botnet were shut down after legal action against them by Microsoft Corp. Authorities severed the Rustock IP addresses, effectively disabling the botnet.

Rustock had been one of the biggest producers of spam e-mail, with some tech security experts estimating they produced half the spam that fills people's junk mail bins.

A botnet is essentially one or more servers that spread malicious software and use the software to send spam or to steal personal information or data that can be used to empty a victim's bank account.

U.S. government programmers shut down the Coreflood botnet on Tuesday. They also instructed the computers enslaved in the botnet to stop sending stolen data and to shut down. A similar tactic was used in a Dutch case, but it was the first time U.S. authorities had used this method to shut down a botnet, according to court documents.

Victims of the botnet included a real estate company in Michigan that lost \$115,771, a South Carolina law firm that lost \$78,421 and a Tennessee defense contractor that lost \$241,866, according to the complaint filed in the U.S. District Court for the District of Connecticut.

The government plans to work with Internet service providers around the

US Shuts Down Massive Cyber Theft Ring

country to identify other victims.

(Reporting by Diane Bartz and Jim Finkle; editing by Gary Hill and Andre Grenon)

US Law Enforcement Agencies Struggle to Detect Cyberattack Sponsors

U.S. law enforcement agencies struggle to detect cyberattack sponsors

BY ALIYA STERNSTEIN 04/13/2011

Most computer crimes originate in Russia and other Eastern European countries, according to U.S. law enforcement officers, but officials do not have the capability to pinpoint whether such attacks are sponsored by criminal enterprises or nation states, they told Senate lawmakers on Tuesday.

Easy, cheap access to the Internet, particularly in that region, has facilitated tax refund scams, ATM fraud and U.S. proprietary data theft, Justice Department officials said during a Senate Judiciary subcommittee hearing on cyber crime.

"Right now, we see on the criminal side a majority of the attacks coming from the individuals who are located in Russia and Eastern European countries," said Gordon Snow, assistant director of the FBI's cyber division. "We see that very large part of the world -- that's extremely connected -- being an area where a lot of the threat is coming from."

Such perpetrators often communicate through chat rooms in a "cyber underground" dedicated to stealing and exploiting identity and financial data, officials testified. Increasingly, they resort to carding, or using a victim's credit or debit card account number -- not only to cash out cards -- but also to sell and resell the identifying data, to hack into other computer systems and commit Internet auction fraud, officials added.

U.S. law enforcement agents have raided many of these communities, yet, as lawmakers underscored, it is hard to determine who or what is stoking the criminal activity.

"China is directing the single largest, most intensive foreign intelligence gathering effort since the Cold War against the United States," said Sen. Orrin G. Hatch, R-Utah. "Methods for conducting informational warfare to advance the goals of the nation state might also involve secretly sponsoring terrorists. China is often cited as providing government support to computer hackers."

The Secret Service, an agency within the [Homeland Security Department](#) authorized to investigate computer crime, two weeks ago obtained a long-term visa to open an office in Beijing, said Pablo Martinez, deputy special agent in charge of the Secret Service criminal investigative division. The Secret Service already has an office in Russia.

Snow said law enforcement and intelligence agencies governmentwide coordinate to try to trace the source of a threat.

"The successes that we've had have been many," he said. "The problem with it is that there are still some very high-profile cases that we've seen, just by looking through *The Wall Street Journal* or

US Law Enforcement Agencies Struggle to Detect Cyberattack Sponsors

any other media outlet, where we still don't know to this day who the attacker is, what state we can attribute it to, or who that person behind the keyboard was."

Snow cited the recent breach of a network owned by the parent company of the Nasdaq Stock Market in New York as an example of the kind of attack directed against important U.S. infrastructure that is difficult to pin to a clear culprit. "As we would in response to any such breach, the FBI is working to identify the scope of the intrusion and assist the victim in the remediation process," he testified.

The cost of cyber crime to the U.S. economy also is hard to decipher. Often, businesses do not disclose attacks, preferring to absorb the cost rather than reveal vulnerability, so it is impossible for officials to accurately quantify the total financial damage. Snow pointed to one [2010 estimate](#) from the Ponemon Institute and security firm ArcSight that calculated the median annual cost of Internet crime for an entity ranges from \$1 million to \$52 million.

Busting the Botnets

Busting the Botnets

The unusual activity generated by zombie computer networks can lead security experts right to them.

By Robert Lemos

They're the scourge of the Internet—networks containing thousands or even millions of virus-infected, remote-controlled PCs. These so-called "botnets" send out spam and launch attacks on websites and computer systems.

But researchers have now come up with a way to spot an infected machine using the way it tries to communicate with its command-and-control server.

Many botnets use a technique known as "domain fluxing" that makes it hard to find and disable the botnet's control server. An infected computer generates a huge list of random-seeming domain names and checks at each domain for the command-and-control server. This makes it difficult for anyone else to know where the botnet controller is. And the creator of the botnet knows how to generate the same list, and only needs to reserve a single domain in order to send commands to the botnet.

In a [recent paper](#), a team of researchers from Texas A&M University and security firm [Narus](#) reveals a way to use domain fluxing to spot a botnet computer. They found that the domains generated by botnets are more random than legitimate ones.

The researchers looked at the domain name queries issued by many different machines. "If the names were closer to a random distribution, we declared them anomalous," says [A.L. Narasimha Reddy](#), a Texas A&M engineering professor who developed the technique with colleagues. A computer that sends requests to 500 domains can be identified as part of the botnet every time.

But Reddy worries that a new, stealthier type of botnet that only wakes up to conduct attacks could make detection harder. "I'm pretty sure that botnet writers will try to innovate by taking measures to defeat the detection," Reddy says. "As long as we have phishing attacks that easily lure people into clicking on links, the attackers will manage to stay ahead."

New legal approaches are helping in the war on botnets. In mid-March, U.S. marshals

Busting the Botnets

and computer forensics experts descended on Web hosting centers in seven U.S. cities, pulling hard drives from servers that were being used to control a massive botnet known as Rustock. The network consisted of over two million PCs being used to send spam.

Microsoft spearheaded the disruption of Rustock by using a trademark infringement law known as the Lanham Act in new ways. By showing that the spammers were using the brands of Microsoft and Pfizer without permission, the companies convinced a judge that drastic measures were necessary. A special legal order allowed Microsoft and the U.S marshals to seize the alleged criminals' hardware without first notifying the owners.

New Pentagon Cyber Strategy Complete

New Pentagon Cyber Strategy Complete: Official

(DEFENSE NEWS 29 MAR 11) ... Marcus Weisgerber

The Pentagon is finalizing a new cyber warfighting strategy that will create a framework for training and equipping forces, as well as call for more international cooperation in this evolving domain, according to a DoD official.

U.S. Defense Secretary Robert Gates is reviewing the document, which could become official in a matter of days, according to Mary Beth Morgan, DoD director for cyber strategy.

"It will help the department better organize, train and equip, and be prepared for its operations across the spectrum - whether it's military, it's business operations, as well as intelligence activities," Morgan said March 29 at an Atlantic Council conference in Washington. "It's a way for us to ensure that we're organizing in the right way, that we're training in the right way, that we're resourcing in the right way."

The cyber warfighting strategy is designed with a "flexible structure so that as this environment and the strategic context changes over time, the department can change and develop over time," Morgan said. The document "gets everybody on the same page and moving forward together so that we do have a more strategic approach to this area," she noted.

A "very large aspect" of the strategy calls for international engagement. This effort will be led by the State Department and help broaden military-to-military relationships, according to Morgan.

"If we as a department are to be successful in defending and providing enhanced security in cyberspace, we must build international partnerships both bilaterally and multilaterally," Morgan said. "It has to be a U.S. government effort in a whole-of-government approach if we're going to be successful."

Building relationships with allies and international partners "to enable information sharing and strengthen collective cyber security" is one of U.S. Cyber Command's top strategic initiatives, U.S. Army Gen. Keith Alexander, the head of the command, wrote in prepared testimony to the House Armed Services Committee on March 16.

The cyber strategy includes engaging the private sector and "the multi-stakeholder forums that help govern and develop the architecture for the Internet," Morgan said.

In addition, the Pentagon has launched a pilot program that uses DoD cyberdefense tools to protect industry networks from attacks, according to a U.S. House lawmaker.

As this initiative takes foot, the government should considering using those tools to defend its infrastructure, according to Rep. Mac Thornberry, R-Texas, chairman of the House Armed Services emerging threats and capabilities subcommittee.

"The pilot program that is just beginning would begin to defend some of the defense industrial, base using those kinds of tools," Thornberry said during a separate presentation at the conference.

Thornberry said there needs to be "cooperation and interrelation between government and private industry," which presents policy challenges, to combat cyber threats.

New Pentagon Cyber Strategy Complete

The Pentagon has been working to streamline its cyber warfighting capabilities for years. In 2009, DoD stood up U.S. Cyber Command as the centralized hub of military cyber operations.

"We ought to look at facilitating the use of the tools that the military uses to defend military networks, to defend critical infrastructure," Thornberry said.

Lawmakers need to update federal policy and laws that have not kept pace with the vast cyber technology advances in recent decades, Thornberry said. House Speaker John Boehner, R-Ohio, has tasked Thornberry with leading a cybersecurity review, which looks at coordinating cyber across a number of congressional committees. A number of panels oversee different cyber efforts.

"As a result, nothing has happened, year after year, after year," Thornberry said.

The congressman said he is optimistic Congress will make advances in developing new cyber policies this year.

But, "while we fiddle, our vulnerability continues to grow," he said.

Cyber Spending at Defense

Cyber Spending at Defense

03/29/2011

In response to a query from Nextgov, Defense officials say they are seeking more than \$3.2 billion in **cybersecurity** funding in 2012 -- that's nearly \$1 billion more than the department first publically reported in February. Here's how the money would be spent:

Cyber Spending at Defense

Army: \$432 million

Information Systems Security Program
\$224M

Defense Industrial Base
\$13M

Other Army Programs
\$195M

Navy: \$347 million

Information Systems Security Program
\$249M

Defense Industrial Base
\$3M

Other Navy Programs
\$95M

Air Force: \$440 million

Information Systems Security Program
\$339M

Defense Industrial Base
\$24M

Public Key Infrastructure
\$39M

Cyber Security Initiative
\$19M

Other Air Force Programs
\$19M

Defense* Agencies: \$1.6 billion

Information Systems Security Program
\$1.076B

Defense Industrial Base
\$19M

Public Key Infrastructure
\$37M

Cyber Security Initiative
\$198M

Other Programs**
\$274M

Other: \$443 million

USCYBERCOM
\$159M

Defense Cyber Crime Center (DC3)
\$26M

Science & Tech Cyber Efforts
\$258M

**Includes DISA, NSA, DARPA, MDA,DLA, DFAS and the Office of the Secretary of Defense.*

***Includes key management infrastructure and other departmentwide programs.*

Cyber Spending at Defense

Source: Defense Department

Virtual War a Real Threat

Virtual war a real threat

The U.S. is vulnerable to a cyber attack, with its electrical grids, pipelines, chemical plants and other infrastructure designed without security in mind. Some say not enough is being done to protect the country.

Reporting from Washington— When a large Southern California water system wanted to probe the vulnerabilities of its computer networks, it hired Los Angeles-based hacker Marc Maiffret to test them. His team seized control of the equipment that added chemical treatments to drinking water — in one day.

The weak link: County employees had been logging into the network through their home computers, leaving a gaping security hole. Officials of the urban water system told Maiffret that with a few mouse clicks, he could have rendered the water undrinkable for millions of homes.

"There's always a way in," said Maiffret, who declined to identify the water system for its own protection.

The weaknesses that he found in California exist in crucial facilities nationwide, U.S. officials and private experts say.

The same industrial control systems Maiffret's team was able to commandeer also run electrical grids, pipelines, chemical plants and other infrastructure. Those systems, many designed without security in mind, are vulnerable to cyber attacks that have the potential to blow up city blocks, erase bank data, crash planes and cut power to large sections of the country.

Terrorist groups such as Al Qaeda don't yet have the capability to mount such attacks, experts say, but potential adversaries such as China and Russia do, as do organized crime and hacker groups that could sell their services to rogue states or terrorists.

Virtual War a Real Threat

U.S. officials say China already has laced the U.S. power grid and other systems with hidden malware that could be activated to devastating effect.

"If a sector of the country's power grid were taken down, it's not only going to be damaging to our economy, but people are going to die," said Rep. Jim Langevin (D-R.I.), who has played a lead role on cyber security as a member of the House Intelligence Committee.

Some experts suspect that the U.S. and its allies also have been busy developing offensive cyber capabilities. Last year, Stuxnet, a computer worm some believe was created by the U.S. or Israel, is thought to have damaged many of Iran's uranium centrifuges by causing them to spin at irregular speeds.

In the face of the growing threats, the Obama administration's response has received mixed reviews.

President Obama declared in a 2009 speech that protecting computer network infrastructure "will be a national security priority." But the follow-through has been scant.

Obama created the position of federal cyber-security "czar," and then took seven months to fill a job that lacks much real authority. Several cyber-security proposals are pending in Congress, but the administration hasn't said publicly what it supports.

"I give the administration high marks for doing some things, but clearly not enough," Langevin said.

The basic roadblocks are that the government lacks the authority to force industry to secure its networks and industry doesn't have the incentive to do so on its own.

Virtual War a Real Threat

Meanwhile, evidence mounts on the damage a cyber attack could inflict. In a 2006 U.S. government experiment, hackers were able to remotely destroy a 27-ton, \$1-million electric generator similar to the kind commonly used on the nation's power grid. A video shows it spinning out of control until it shuts down.

In 2008, U.S. military officials discovered that classified networks at the U.S. Central Command, which oversees military operations in the Middle East and Central Asia, had been penetrated by a foreign intelligence service using malware spread through thumb drives.

That attack led to the creation in 2009 of U.S. Cyber Command, a group of 1,000 spies and hackers charged with preventing such intrusions. They also are responsible for mounting offensive cyber operations, about which the government will say next to nothing.

The head of Cyber Command, Gen. Keith Alexander, also leads the National Security Agency, the massive Ft. Meade, Md.-based spy agency in charge of listening to communications and penetrating foreign computer networks.

Together, the NSA and Cyber Command have the world's most advanced capabilities, analysts say, and could wreak havoc on the networks of any country that attacked the U.S. — if they could be sure who was responsible.

It's easy to hide the source of a cyber attack by sending the malware on circuitous routes through computers and servers in third countries. So deterrence of the sort relied upon to prevent nuclear war — the threat of massive retaliation — is not an effective strategy to prevent a cyber attack.

Asked in a recent interview whether the U.S. could win a cyber war, Alexander responded, "I believe that we would suffer tremendously if a cyber war were conducted

Virtual War a Real Threat

today, as would our adversaries."

Alexander also is quick to point out that his cyber warriors and experts are legally authorized to protect only military networks. The Department of Homeland Security is charged with helping secure crucial civilian infrastructure, but in practice, the job mostly falls to the companies themselves.

That would've been akin to telling the head of U.S. Steel in the 1950s to develop his own air defenses against Soviet bombers, writes Richard Clarke, who was President George W. Bush's cyber-security advisor, in his 2010 book, "Cyber War: The Next Threat to National Security and What to Do About It."

The comparison underscores the extent to which the U.S. lacks the laws, strategies and policies needed to secure its cyber infrastructure, experts say.

"If we don't get our act together, the consequences could be dire," said Scott Borg, who heads the U.S. Cyber Consequences Unit, which analyzes the potential damage from various scenarios.

The problem, though, is "there's nothing that everyone agrees on," said James Lewis, cyber-security expert at the Center for Strategic and International Studies in Washington.

For example, Lewis and other experts believe the government should mandate cyber-security standards for water systems, electric utilities and other crucial infrastructure. Some contend that major U.S. Internet service providers should be required to monitor patterns in Internet traffic and stop malware as it transits their servers.

But both ideas are viewed with suspicion by a technology industry that wants the government out of its business, and by an Internet culture that sees such moves as

Virtual War a Real Threat

undermining privacy.

"There are a whole lot of things that can't be legislated," said Bob Dix, vice president of government affairs for Sunnyvale, Calif.-based Juniper Networks Inc., which makes routers and switches.

Yet Washington may be reaching a moment when the seriousness of the threat trumps political resistance. Sources familiar with the negotiations say the White House has promised Senate leaders that it will offer its own cyber-security legislation in a month. But any proposal that calls for far-reaching regulations would face an uphill battle.

CIA Director Leon E. Panetta told Congress recently that he worried about a cyber Pearl Harbor. Yet many who follow the issue believe that's what it will take to force Americans to awaken to the threat.

"The odds are we'll wait for a catastrophic event," said Mike McConnell, former director of National Intelligence and cyber-security specialist, "and then overreact."

What a Cyber War with China Might Look Like

What a cyberwar with China might look like

Former U.S. diplomat describes hypothetical scenario

By Jaikumar Vijayan

March 31, 2011 06:00 AM ET

Computerworld - It's August 2020. A powerful and rising China wants to bring the city-state of Singapore into its fold as it has with Hong Kong, Macau and Taipei.

Its first physical attacks against Singaporean assets are still weeks away. But already, China has launched a massive cyber campaign, designed largely to degrade and disrupt the communications capabilities of the U.S., Japan and other allied nations.

Members of the Chinese military's 60,000-strong cyberwarfare group have deeply penetrated U.S. military, government and corporate networks and are already manipulating and controlling them.

When the Chinese army finally launches its first attack against a Singaporean guided missile frigate in the South China Sea in September, U.S. armed forces find their communications capabilities severely compromised. Personal computers, radios, satellite communications capabilities and battlefield communication hardware are all but crippled.

Key military networks and servers come under crushing denial-of-service (DoS) attacks, hampering the Pentagon's efforts to mobilize conventional forces. Deliberately injected misinformation flows over the networks to field commanders and to ships at sea.

What a Cyber War with China Might Look Like

The conflict ends 55 days later in a standoff between the U.S and the Chinese navy, with a general war being avoided and Singapore retaining its independence.

That's a hypothetical scenario of how a truly full-scale cyberwar launched against the U.S by China would play out, and it's very different from the way [many expect such a confrontation look like](#).

The scenario is described in detail in a report in the latest issue of the U.S. Air Force's Strategic Studies Quarterly ([download PDF](#)). The report was authored by Christopher Bronk, a former diplomat with the U.S. Department of State and a fellow specializing in IT policy at Rice University's Baker Institute.

The scenario depicts just one way in which a cyberwar could unfold and is designed to highlight how such conflicts are very unlikely to be a bolt from out of the blue.

"Most likely, cyber conflict will be an 'always on' engagement, even if international policy is enacted to forbid it," Bronk writes in the article. "The only certainty in cyber conflict is that conflict there will not unfold in the ways we may expect."

Speaking with *Computerworld* this week, Bronk downplayed popular perceptions of a cyber Pearl Harbor, in which critical infrastructure targets such as the electrical grid are attacked and taken out.

Such attacks can't be ruled out entirely, but it's unlikely that a nation state would launch one because of the catastrophic response it would trigger.

"I did not try to make the case that it would be some sort of an apocalyptic event. I did not make the case that it would occur in isolation," he said. Instead, a cyberwar will most likely be part of a broader war or broader campaign, as cyberattacks were

What a Cyber War with China Might Look Like

part of more conventional conflicts in Georgia and Estonia, he said.

As tactics employed as part of a larger war, cyberattacks will be designed to degrade and disrupt communications and will be terribly hard to thwart, Bronk said. The goal will be not so much to completely disable an opponent's networks but to own as much of a network as possible in order to control it when hostilities break out, he said.

The effort will be "to get inside the other guy's decision process rather than shutting it off entirely," Bronk said. "You don't want your adversaries to abandon their information technology."

In Bronk's hypothetical scenario, for instance, China's cyber offensive is noisy and highly visible but also extremely disruptive. The attacks aren't targeted just at highly secure and classified U.S. networks.

Instead, China's cyber army deeply penetrates many of the unclassified networks used by the government and the military for relatively low-level internal communications and for tasks such as routing supply information.

"Although unclassified, when aggregated, the information passing across these networks provided highly useful intelligence to the Chinese on U.S. dispositions and strategy," Bronk writes in his report. The data gleaned from such networks can provide adversaries with a detailed look at troop movements, cargo operations and demand for fuel and other basic supplies.

In Bronk's scenario, Chinese cyberwarriors penetrate the networks of U.S. corporations' China-based operations long before the conflict starts, and when the fighting begins they use information from those networks to add to the chaos.

What a Cyber War with China Might Look Like

False information is deliberately injected into the corporate systems. Package carriers such as FedEx and UPS are forced to halt operations because their systems are routing packages everywhere except to the correct destinations.

"For defense planners at the Pentagon, it was hard enough to know what U.S. forces were doing, let alone the enemy," he writes. "Ships at sea in the Pacific encountered all manner of navigation and datalink issues."

Bronk says his scenario is just one way a cyberwar is likely to play out. But one thing he is relatively sure of is that such a war, if it happens, will not necessarily involve power grids being knocked offline and planes falling from the sky.

To counter the attacks, the U.S. will have to muster all available resources from the NSA, the Homeland Security Department, the DISA, the CIA, the State Department, the Department of Justice and other agencies. Also joining the operation would be top theoretical staff, engineers and even linguists from academia and other specialists from the private sector.

And even then it would take several weeks to disassemble the Chinese attacks, mount a defense against them and re-establish trust in U.S. networks and systems.

However, Bronk said, "I don't see these cascading sets of attacks, where by the end of Day Three we are all sitting in darkness eating beans and heading out into the mountains with our guns."

Unconventional Methods Needed to Recruit Cyberwarriors

Industry: Unconventional Methods Needed to Recruit Cyberwarriors

NATIONAL HARBOR, Md. — When looking for fresh talent, the nation's largest government contractors often head to prestigious universities to recruit high-performing students with top GPAs.

But that's not where they will find the best minds that they need to tackle cybersecurity threats, said Lynn Dugle, president of Raytheon's intelligence and information systems division. The names of the individuals whom industry needs may not even make it on a diploma, she said.

Of the last three premier cyber-related hires her company has made, none had a college degree. One was a high-school dropout who stuffed pills into bottles at a pharmaceutical plant by day and dominated hacking competitions at night.

"We're looking for talent in all of the wrong places," Dugle said during a March 31 panel discussion at the Air Force Association's CyberFutures symposium. Companies, she said, are not helping themselves by failing to become attractive places of employment for the talented individuals they seek.

Large companies are perceived as being too conventional — with strict workday schedules, dress codes, and management structures that reward those who climb up the corporate ladder. This doesn't mesh with the lifestyle of many individuals with the hands-on knowledge and experience operating in cyberspace, Dugle said. She said industry should turn things upside down and offer straightforward incentives in a true pay-for-performance scheme. "For every vulnerability you solve, I'll cut you a check," she said. "I don't care if you're in the office or not."

Industry also is relying too much on antiquated training methods, Dugle said. "In this field, dynamic learning is the name of the game."

At Northrop Grumman, employees are expected to have a basic understanding of cybersecurity issues, said Robert Brammer, vice president for advanced technology. Beyond the basics, the firm runs an internal cyber academy. About 1,000 employees are expected to complete the course this year, with more scheduled to attend in future years.

These activities are aimed at turning cybersecurity work from a niche to a

Unconventional Methods Needed to Recruit Cyberwarriors

mainstream career path. And that will happen, said Barbara Fast, vice president of cyber and information solutions at Boeing Network and Space Systems. Eventually, there will even be an Air Force chief of staff who will also be a cyberwarrior, she said. Fast called U.S. Cyber Command's leader Army Gen. Keith Alexander the first in what will be a long line of "cyber seniors" in the military and industry, she said.

Agencies also must continue to improve ways to identify talent, industry executives said. It's not enough to look at someone's resume, Fast found out when she recently asked a U.S. Naval Academy midshipman what he considered the most important competency for a cyberwarrior. "A devious mind," he said.

Iran Accuses Siemens Over Stuxnet Virus Attack

Iran accuses Siemens over Stuxnet virus attack

TEHRAN | Sun Apr 17, 2011 7:48am EDT

(Reuters) - An Iranian military commander has accused German engineering company Siemens of helping the United States and Israel launch a cyber attack on its nuclear facilities, Kayhan daily reported on Sunday.

Gholamreza Jalali, head of Iran's civilian defense, said the Stuxnet virus aimed at Iran's atomic program was the work of its two biggest foes and that the German company must take some of the blame.

Siemens declined to comment.

"The investigations show the source of the Stuxnet virus originated in America and the Zionist regime," Jalali was quoted as saying.

Jalali said [Iran](#) should hold Siemens responsible for the fact that its control systems used to operate complicated factory machinery -- known as Supervisory Control and Data Acquisition (SCADA) -- had been hit by the worm.

"Our executive officials should legally follow up the case of Siemens SCADA software which prepared the ground for the Stuxnet virus," he said.

"The Siemens company must be held accountable and explain how and why it provided the enemies with the information about the codes of SCADA software and paved the way for a cyber attack against us," he said.

Some foreign experts have described Stuxnet as a "guided cyber missile" aimed at

Iran Accuses Siemens Over Stuxnet Virus Attack

Iran's atomic program.

Unlike other Iranian officials who have played down the impact of Stuxnet, Jalali said it could have posed a major risk had it not been discovered and dealt with before any major damage was done.

"This was a hostile act against us which could have brought major human and material damages had it not been encountered promptly."

Iran has given few details of the impact of the virus. It said in September that staff computers at the Russian-built Bushehr nuclear power station had been hit but that the plant itself was unharmed.

Bushehr -- Iran's first nuclear power station -- is still not operational, having missed several start-up deadlines, prompting speculation that it too had been hit by Stuxnet, something Iran denies.

Russia's ambassador to NATO said in January the virus had hit the computer system at Bushehr, posing the risk of a nuclear disaster on the scale of the 1986 Chernobyl incident in Ukraine, then part of the Soviet Union.

Some defense analysts say the main target was more likely to be Iran's uranium enrichment -- the process which creates fuel for nuclear power plants or provide material for bombs if processed much further. Western powers accuse Iran, a major oil producer, of seeking to develop nuclear weapons capability, something Tehran denies.

U.S.-based think-tank, the Institute for Science and International Security (ISIS), said that in late 2009 or early 2010 about 1,000 centrifuges -- machines used to refine uranium -- out of the 9,000 used at Iran's Natanz enrichment plant, had been knocked out by the virus -- not enough to seriously harm its operations.

Iran Accuses Siemens Over Stuxnet Virus Attack

(Additional reporting by Jens Hack in Munich; Writing by Ramin Mostafavi; Editing by [Robin Pomeroy](#) and [Janet Lawrence](#))

Federal IT Professionals to Receive New Program Manager Status

Federal IT professionals to receive new program manager status

BY ALIYA STERNSTEIN 03/30/2011

The Obama administration has proposed creating a new federal position -- information technology program manager -- to help reverse the multiyear delays and multimillion-dollar losses that agency computing projects traditionally accrue. The new position is part of a [25-point strategy](#) unveiled late last year for changing the way the government buys IT systems and services.

The [Office of Personnel Management](#) on Tuesday issued a [draft job description](#) for the new title. The position's responsibilities include coordinating, communicating and integrating IT projects and program activities; ensuring such work achieves the outcome specified by IT business strategies; and conducting negotiations and decision-making to execute programs.

The post involves managing at least one "large" IT program "to provide products and/or services." A project is a singular endeavor with a tangible outcome that starts and stops during a short period of time, whereas a program typically consists of several interrelated projects aimed at achieving a certain long-term benefit for the agency.

IT program manager will be added to a category of jobs known as the IT Management 2210 series. All jobs in the series require knowledge of information technology concepts, including data storage, software applications and networking. Other positions in this class include project manager and IT specialist.

Establishing a career path for IT program managers is the centerpiece of the technology management overhaul, which also focuses on centralizing purchasing power at the office of the chief information officer, increasing communication with potential vendors early in the bidding process and outsourcing IT services to online hardware and software providers in the cloud.

Eventually, programs will be denied funding unless they are staffed by a dedicated program manager, according to the plan. The White House has instructed OPM to design a formal IT program management career roadmap by June that includes direct hiring authority. Agency officials currently are consulting with subject matter experts to develop a competency model for IT program managers and will survey federal employees for feedback in April, according to administration officials.

Bolstering program management is one of the least controversial IT reforms, but funding for education, new jobs and promotions might be hard to get from Congress in a tight economy. Administration officials said previously that they expected to provide \$158 million in fiscal 2011 for training and hiring civilian acquisition professionals.

Federal IT Professionals to Receive New Program Manager Status

Program management enthusiasts said the discipline will be attractive to youth entering the federal workforce because it involves heading up major initiatives, such as FBI information sharing, that effect change in government.

An announcement about the new title on the CIO.gov federal website, stated, "The government is taking steps to recruit talent with deep experience in IT management, who can take ownership and 'steward IT programs from beginning to end.' The IT program manager title is a step toward recruiting the best of the best for these critical roles."

Interested members of the public and employees have until April 14 to comment on the new title.

Rapid Fielding Should Increase as Military Borrows from Private Sector

Rapid Fielding Should Increase As Military Borrows More From Private Sector

(SAN DIEGO DAILY TRANSCRIPT 29 MAR 11) ... Elizabeth Malloy

The U.S. military prides itself on being both the most technologically advanced fighting force on earth, as well as the quickest to respond to any emergency. Unfortunately, those two concepts don't always mesh.

Getting a product to soldiers and sailors as quickly as possible is known in the military as rapid fielding, but "rapid" in this context doesn't mean what it often does in the rest of the world. While technology is changing every few months, regulatory hoops and other issues can mean that new software can take years to be installed on a Naval ship, by which time it's practically outdated.

To solve this problem, Rear Adm. Patrick Brady, commander of SPAWAR, said that the military needs to look at its acquisitions process to create what he called a "left-hand lane" to speed up the acquisition and deployment of certain technologies.

"For this high priority issuing, this left-hand lane, you follow this new, faster set of rules," Brady explained. "Maybe you're addressing things by ship class, or by individual ships, that let you go through that."

Brady was speaking at a recent Daily Transcript roundtable, co-hosted by the San Diego chapter of the National Defense Industry Association, which brought together local Navy leaders, and representatives from defense contractors.

Brady said that the Navy wants to incorporate a faster way to get tools into the hands of its soldiers, but it must sort out the rules. Who, for example, would decide which products are fast tracked? Organizations such as the U.S. Cyber Command, a subordinate to the branch-wide U.S. Strategic Command, prioritizes which software systems must be replaced with more advanced versions, but choosing which advanced version goes into effect is a different matter.

Brady said this responsibility would likely fall to the commander of the Tenth Fleet, which since its founding in World War II, has been on the Navy's cutting edge.

Leaders from the defense industry said that they noticed some areas of the military's acquisition process that could be altered to make it easier to get high-tech products onto ships and bases quicker. Dennis Bauman, an independent consultant who spent 30 years in the government's senior executive service, said that the Department of Defense uses the same acquisition process for hardware as software, and they're really different products.

"We in the acquisition field in the DOD have DOD Instruction 5,000, that series of acquisition regulations which many of you in this room know very well, and it's a one size fits all set of statute, regulation policy," Bauman said. "After years of treating a radio program like a ship building program in terms of what you have to do inside the building to move forward with it, I've become convinced that we need a different DOD 5,000 for C4I (Command, Control, Communications, Computers and Intelligence) than we have for many of the other weapons systems."

Industry leaders said they would also like to see more communication between the military and

Rapid Fielding Should Increase as Military Borrows from Private Sector

the private sector over what, exactly, is needed. Duane Roth, chief executive officer of the trade group Connect, said that San Diego is a leader in finding ways to rapidly mine large amounts of data and find the information needed to make decisions, for example, but often private sector companies aren't sure how to get a contract with the department of defense.

"We don't know your vocabulary, we just don't. We don't understand how to do business with you," Roth told Naval leaders. "But we have solutions. And vice versa, you have things that we'd very much like to bring into the commercial world, but we don't know what those are."

Capt. Joe Beel, commander of SPAWAR Systems Center Pacific, said that he would like to see more programs that bring sailors directly into laboratories, so they can tell researchers what kinds of tools they need. This could also lead to more rapid fielding, and needs would be more directly met.

As the military borrows more and more from the private sector, where platforms such as the one used by Apple on its iPhone are becoming more commonly adapted, rapid fielding should increase. Under that platform, it's easier to plug new applications into an existing hardware system, rather than replacing the whole system when there is a need for a new program. Both Navy and industry leaders pointed to the Consolidate Afloat Networks and Enterprise Services program (CANES), a system used on many ships, as successful example of this.

This requires long-term planning, as platforms need to have the memory capabilities to host the systems of the future. Long-term planning in the military is difficult because budgets change yearly and are subject to political necessities.

Roth, however, said that he felt like the niches San Diego's technology companies have become known for, such as wireless and data mining solutions, are a great fit for the military's needs, and the more collaboration the better.

"If there was ever a living laboratory in this country, it's here," he said.

F-22s Won't Get F-35 Datalinks Yet

F-22s Won't Get F-35 Datalinks, Yet

By [John Reed](#) Thursday, March 31st, 2011 1:58 pm

Air Force leaders shed more light on the communications issues facing the F-22 Raptor today, telling lawmakers that the plane will not be receiving the same datalink being developed for the F-35 Joint Strike Fighter.

The service had been looking at integrating the Multifunction Advanced Datalink onto the F-22, F-35 and B-2 Spirit bombers in an effort to give all stealth jets a secure way of communicating.

MADL however, is not "mature" enough to install on the Raptor without incurring too much risk, said Air Force Chief of Staff Gen. Norton Schwartz.

"We should let the F-35 development effort mature before tacking it onto the F-22, this was a cost and a risk calculation on our part," the four-star told the House Appropriations defense subcommittee today.

He went on to say that the jet "can communicate" with older fighters using Link-16 via something called BACN, a version of which can translate info from the Raptor's Intra-flight Data Link to Link-16 format; allowing it to communicate with older fighters. BACN has been critical in aiding communications in the skies over Afghanistan where it's been mounted on everything from a Block 20 RQ-4 Global Hawk to business jets. ([Here's](#) a more detailed explanation of these so-called communications gateways.)

However, when asked if the version of BACN that allows the Raptors to actually talk to other jets has been fielded, Schwartz couldn't say.

So yes, in theory, the Air Force has a tool that can allow the F-22 to communicate with Link-16 equipped jets. In reality, it may not be fully fielded yet in sufficient numbers. The way Schwartz described it, anytime the F-22 would deploy with other fighters, it would need a RQ-4 Global Hawk drone equipped with BACN to be loitering nearby.

While the Air Force insists the jet wasn't used in Libya [because it is based too far from the fight](#), some speculate that its inability to communicate with other fighters is the real reason it was left out of Operation Odyssey Dawn.

So, given the fact that the F-22 is based far from Libya combined with the fact it would take the deployment of a Global Hawk equipped with a gateway, that may or may not be fielded, to allow it to talk to other jets, it seems like the communications issue may have played a role in the service's decision to exclude it from Libyan ops. It would just be too much effort to quickly deploy the Raptor, a jet which wouldn't have a heck of a lot of use in Libya, with its ancient air defenses, to begin with.

F-22s Won't Get F-35 Datalinks Yet

Military Scouts Best Ways to Protect Stored Data

Military scouts best ways to protect stored data

Encryption, solid-state drives hold most promise

- By [Henry Kenyon](#)
- **Apr 01, 2011**

Information security in the predigital age involved physical barriers, locks and guards. Modern data systems are more secure — yet also more vulnerable — than the acres of file cabinets they replaced.

The Defense Department has spent a lot of time and money on technologies to keep its classified and unclassified content secure. The need to protect that information now and migrate it to new systems in the future influences DOD's acquisition decisions.

The primary agency responsible for managing, storing and securing military data is the Defense Information Systems Agency. One of DISA's major challenges is dealing with massive amounts of information across a range of security classification levels, said Kerry Miller, branch chief of DISA Computing Services' engineering design group in Denver, Colo.

DISA has turned to a variety of technologies, such as systems with built-in encryption, to deal with that security problem. Miller said several vendors incorporate encryption in their hardware, which then eliminates the need for external encryption/decryption systems. Built-in encryption can protect data on physical media such as hard drives and laptops. If a portable device is stolen or lost, the data remains protected and is difficult to extract, he said.

Built-in encryption also protects data from equipment failure. If an unencrypted disk that contains classified information goes bad, an adversary might still be able to retrieve at least some data. Miller cited the example of a disk containing payroll data. A thief might not be able to read the entire disk but could still access a few Social Security

Military Scouts Best Ways to Protect Stored Data

numbers.

But by encrypting data on the hardware as it is recorded, the information will be much harder to access if it falls into the wrong hands, Miller said. That is important to DISA because the agency works with classified and unclassified but sensitive data, such as payroll information and medical information, on its networks.

Tagging and migrating data

DISA also is looking at data tagging for storage media. Tagging allows users with certain privileges to access specified data. Miller expects data-tagging technology to become more powerful and efficient, which would greatly enhance security.

Miller said access authentication problems are “probably the bane of our existence today.” He said authentication was not previously viewed as a major problem, but recent threats such as identity theft and terrorism coupled with the prevalence of more open and accessible processing platforms create more concerns. “Today, with a few thousand dollars at home, anybody can potentially tap into your environment and steal your information,” he said.

Older media also remains a problem. Miller said DISA Computing Services regularly migrates data to new storage technologies and works to eliminate data that no longer has any value. But he added that the agency must store important information to satisfy regulatory or mission requirements. “We’ve actively worked with our customers over the years to migrate that data to the newer form factors,” he said.

Miller said that when DISA designs computer systems, redundancy and security are built into them as standard procedure. Storage systems also are segmented among applications to separate data types, and classified systems are detached from unclassified information. DISA also has media destruction contracts with vendors to eliminate old or defective storage media.

DISA also has an aggressive technology refresh program to keep information up to the latest standards. “We try not to be on the bleeding edge because, being on the bleeding edge, you tend to fight through a lot of problems and you’re...debugging

Military Scouts Best Ways to Protect Stored Data

systems for the vendor community,” Miller said. The agency waits until a technology is proven in the marketplace. However, he said DISA tries to refresh its technology every three to four years to keep up with the latest technology.

Navy moves to secure its data

Another example of an enterprisewide DOD network with data storage security needs is the Navy Marine Corps Intranet. As the Navy’s primary IT network, NMCI has been at the forefront of developing and implementing security technologies and initiatives, said Capt. Shawn Hendricks, program manager of naval enterprise networks.

In February 2007, NMCI began a series of 16 major information assurance programs to fix known security deficiencies and keep pace with rapidly growing cyber threats. The programs used an approach that applied layered security mechanisms to protect the network. Hendricks said that method extends across the NMCI infrastructure, from the network perimeters to server farms and users' workstations. One of those capabilities is a data-at-rest (DAR) program deployed to all NMCI users to increase the security of their data, files and folders.

The DAR deployment began in February 2008. Hendricks said it consists of an encryption security system provided by Symantec, which acquired the system from GuardianEdge Technologies. The system ensures users comply with DOD and Navy mandates designed to protect data at rest. The capability also reduces the risk of unauthorized access to data. The DAR program includes full-disk encryption of hard drives and removable storage encryption. He said NMCI's DAR system can scan 1 quintillion keys per second for security. “An attacker would require [thousands of] years to successfully defeat the disk encryption key,” he said.

The DAR encryption operates in the layer between a computer’s operating system and physical disk. Supporting disk management utilities can't bypass the DAR system to directly modify a disk or the data will be lost and the hard drive damaged. For example, if an encrypted hard disk is repartitioned using standard utilities, the utility must account for the DAR system or risk overwriting critical DAR file tables and breaking the drive, Hendricks said. He said that this example demonstrates that important

Military Scouts Best Ways to Protect Stored Data

improvements remain before the DAR system can be seamlessly integrated with disk management utilities. “In the near term, where automated protections are yet to be developed by the DAR vendor, NMCI employs other processes to ensure compliance,” he said.

The Navy also is evaluating the pricing and development of solid-state drives and self-encrypting drives, said Dennis Hayes, chief technologist for the enterprise services division at Hewlett Packard’s U.S. defense business, which supports NMCI. However, there are some complications with the technology. He said although self-encrypting drives move the encryption process to a drive's firmware, it introduces issues with key management. For example, because the GuardianEdge software has a coupled server and client component that communicate with each other to approve keys, a drive is unreadable if a key gets lost.

“With hardware-based encryption, it’s unclear which key management scheme we could use, whether we could continue with the one we have or would we be looking at a generalized key management scheme that would be managing keys for all sorts of things — not just hard drive keys,” he said.

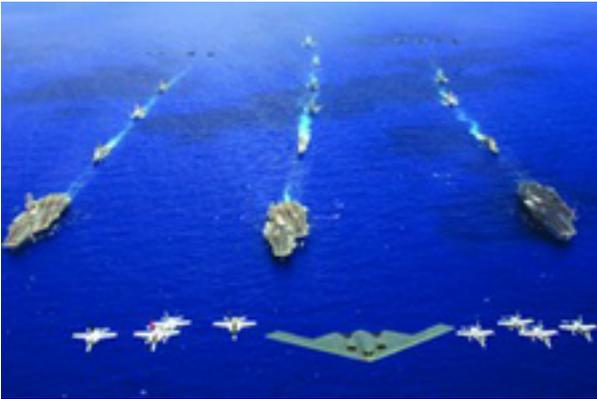
Hayes said solid-state drives need to become less expensive before the Navy can buy them in bulk. He said those drives manage data differently from rotating drives because they use flash memory to move stored data to the upper file system. However, the Navy is unsure about how robust a software encryption scheme needs to be for such drives given that the firmware in the drive is moving the data, he said.

AirSea Battle Concept Is Focused on China

AirSea Battle Concept Is Focused On China

By Bill Sweetman, Richard D. Fisher, Jr.
Washington, Washington

AirSea Battle Concept Is Focused on China



U.S. Defense Secretary Robert Gates says it has the “potential to do for America’s military deterrent power . . . what AirLand Battle did” in the 20th century.

The chief of naval operations sees it as paradigm-shifting. “I don’t want to be over the top,” Navy Adm. Gary Roughhead said at an Aviation Week conference in February, “but it’s pretty ground-breaking.”

What has these men seemingly so excited? The answer: The nascent AirSea Battle concept now being hammered out by Air Force, Navy and other defense officials inside the Pentagon and elsewhere. But while this high-profile joint battle plan may be the vanguard of U.S. operations for this century, questions linger over whether it is even keeping up with the threats known and otherwise.

It is no revelation that long-term U.S. Air Force and Navy planning is focused on China. But while some innovations are underway, like the unmanned combat aerial system (UCAS), U.S. options in response to Chinese threats largely do not include the rapid development and deployment of major new weapons, especially with limited research, development and procurement resources under increasing budget pressure. The emerging AirSea Battle concept, consequently, relies on the reorientation of current programs and the use of networking to ensure freedom of operation in anti-access/area denial (A2/AD) environments.

The Washington-based Center for Strategic and Budgetary Assessments (CSBA) has issued some of the more detailed, public documents behind AirSea Battle thinking. (Former CSBA analysts, including now-Deputy Navy Secretary Robert Work, occupy key positions in Washington.) CSBA’s most comprehensive report stresses that “AirSea Battle, as a doctrine for the operational level of war, cannot and should not be seen as a ‘war-winning’ concept in itself. Nor should it be viewed through the lens of a particular scenario, for example, the defense of Taiwan. Instead, it should be considered as helping to set the conditions at the military operational level to sustain a stable, favorable conventional military balance throughout the Western Pacific region.”

So it is not about fighting China, but maintaining a military balance to sustain stability in the region—but it is a military concept for combat operations, which responds to visible Chinese

AirSea Battle Concept Is Focused on China

'We're Not Gambling'

(*AVIATION WEEK & SPACE TECHNOLOGY 04 APR 11*) ... Amy Butler and Anthony L. Velocci, Jr.

As the Pentagon celebrates the Centennial of Naval Aviation this year, its top officer is shepherding many new technologies into its carrier air wings, including unmanned aircraft and the Joint Strike Fighter. Last month, Chief of Naval Operations Adm. Gary Roughead discussed his plans for naval aviation with Editor-In-Chief Anthony L. Velocci, Jr., and Senior Pentagon Editor Amy Butler at his Pentagon office.

AW&ST: Do you expect the threats the Navy will face in the next decade to be markedly different or greater than what the Navy has faced since the Cold War?

ROUGHEAD: They will be greater. I think that's just the nature of how technology and warfare progresses. If you go back in naval aviation to the advent of the aircraft carrier, people thought 'this isn't going anywhere.' And in World War II, in particular, the role of the carrier changed things. The biggest change [ahead] is in the information space and how you operate in there. In that battlespace, the Joint Strike Fighter (JSF) will be one of the best sensors . . . and a very lethal one.

Given this evolving threat environment, what is the Navy's overarching strategy?

This past weekend [March 19-20], you saw the maritime strategy in full play off the coast of Libya—sea control, power projection. Plus, we have our deterrent force on patrol all the time around the world. The two carriers that are at sea in the Middle East are also a deterrent force, for anyone that's thinking about any kind of mischief there.

How might carrier operations change in the coming years?

The first change will be with the introduction of unmanned aircraft and the Joint Strike Fighter. [They will bring] a new means to interface and interact with the airplane not only in the air, but also on the ship itself. As I look at the introduction of JSF, in particular, I've really been pressing my folks on how that airplane interfaces with the ships from which it will operate.

Would you elaborate on exactly what you mean?

If you employ the JSF like you have fought everything else, then you are not going to be getting the full advantage of the airplane. There are huge amounts of information that will be made available from the F-35. How does that interface into the ship systems? It's not simply the operational or the tactical information; it's also all of the information about the health of the airplane. So how do you learn to take advantage of that type of technology and everything that's displayed? That is why it is so important for me to get that ship-airplane interface down. We can buy a great airplane, but if we don't have the ways in which we're going to fly a weapon system and move the information, it will be sub-optimized.

How rapidly do you expect unmanned naval aviation to evolve?

'We're Not Gambling'

You are not going to see unmanned aircraft operating tactically anytime soon. But I have put a marker down that I want a squadron of unmanned vehicles operating on aircraft carriers by 2018. A lot of people have told me that is pretty aggressive. My answer to that is, 'Tough.' In 2018, I want to have that capability operating so that we can learn from it.

Do you see the day when there will be a carrier-based wing that is completely unmanned?

You know that line: 'Never say never.' But, I do not [anticipate] it in the foreseeable future. The next generation of naval officers—those who are about to graduate this spring—will see a mix of manned and unmanned airplanes operating on carriers.

The Unmanned Carrier-Launched Airborne Surveillance System (Uclass) is intended for service in 2018. Will that weapon system need to be a tailless aircraft?

I want to go to a low-observable form. I think it is important not just for survivability, but also to have the technology that will allow us to fly that [weapon system] off of an aircraft carrier. The aerodynamics are going to be a little bit different. To do an interim step just prolongs the process, [although] I also believe [going tailless] has the potential to cost us more money. The unmanned combat air system demonstrator (UCAS) that exists today flies pretty well. There are some people who would say, 'Let's just take some of the existing non-low observables and convert those to our maritime application.' I think we would be missing an opportunity. I believe we should jump, and we should move fast.

What is your vision for unmanned rotorcraft?

The Navy has a lot of airfields, some of them no bigger than this [office]. We are going into rotary-wing because we have to be able to set down in very small spots. That is why you are seeing Fire Scout. Then we plan to transition into the medium-range UAS, which will be a rotary as well. But, once we put them in the hands of our sailors, they come up with better ways to do the job. As these systems are introduced, you will see some terrific innovation take place. And that is why it's so important for me to get unmanned aerial systems out there in the hands of operators. [Just] flying them around the Pentagon on PowerPoint does nothing for me.

How are new and recently introduced weapons systems doing in the Libya conflict?

The Navy picked up the electronic-attack function. The original plan was for the EA-18G Growlers to first go to sea as part of air wings. But last year, I said we will push the Growlers into the expeditionary squadrons first, because I wanted to get them into the fight. We had our first Growler [combat] deployment in Iraq. Just 47 hours after they recovered from flying combat missions there, they were launching on the Libyan mission from Italy. Also, the fact that we had an MV-22 Osprey on board allowed us to rescue the crew of the downed Air Force [F-15E] airplane [on March 22]. That was a fortuitous pairing to have MV-22 there because of its speed. It showed us the value of that airplane. This was also the first combat use of the SSGN, the converted ballistic missile submarine, employing a pretty healthy load of Tomahawks.

China reportedly has deployed a so-called aircraft carrier killer. Does such a weapon upset the balance of power insofar as the Navy is concerned?

No. You have to look at the total employment of the weapon. You have to look at the nature of

'We're Not Gambling'

being able to first locate, then target, and then engage a moving sea-borne target at range. I'm always struck at how captivated people have gotten about the carrier killer. Nobody's talking about the precision with which every fixed airfield in the region could be targeted. I really do think that it is not the game-changer people have played it up to be.

As naval aviation evolves from the F/A-18E/F to the F-35, will the Navy take on additional risk during this transition period?

We are operating under a bit of risk. We have 150 Hornets, which we will put into a service-life-extension program for which we have set money aside. Then we are going to procure the 41 additional Super Hornets. I believe our deployed airpower will be in a very good position. But, there is a little bit of what we call a strike fighter shortfall, which will require more energetic management in making the airplanes available.

What are your immediate budget concerns?

There has to be a commitment to how you minimize the cost per flying hour, and how you make sure you are flying the appropriate numbers of hours to maintain operational and combat proficiency without doing anymore than is [necessary]. That is going to be a great challenge for us as we go forward, and it will require leadership who can think anew about how to accomplish this goal. As increased technology is pursued, we will come up short unless we are entering that pursuit with total ownership costs in mind from the beginning.

One of the areas that I've addressed with my staff and leadership on numerous occasions is that you can really be seduced by unmanned technologies. And you get the sense that if you're doing something in the unmanned world, somehow people are not involved. Well, if you don't control who is in the back room, you are not going anywhere as far as total ownership cost goes.

As we have pursued our unmanned program, one of the first questions I always ask is about manpower. It is the most expensive cost, but often it is at the very tail end of the decision process. You come up with this wonderful technological solution, and then in the last five minutes of the meeting somebody says, 'Oh, by the way, you'll have to produce 400 more people for it.'

How do you view the future for naval aviation in the near-term?

Everything coming in is new. And the best thing about it is that it's all flying; it's not some idea that we have for the future. The Joint Strike Fighter is flying at Pax [NAS Patuxent River, Md.]. The P-8 is flying at Pax. UCAS is flying in California. Fire Scout is deployed. Growlers are in combat, and the UH-60s [Black Hawk helicopters] are deployed. You can touch everything we have going forward. In other words, we are not gambling. We're still in the testing program on the F-35C, but in my mind, we're not gambling. The F-35C is going to be a good airplane, and everything else is brand-new.

If I was a young aviator coming into the Navy today, I would think the future is pretty exciting.

Soldiers' Wearable Computers May Get an iPhone Brain

Soldiers' Wearable Computers May Get an iPhone Brain

- By [Spencer Ackerman](#)  April 14, 2011 | 2:35 pm | Categories: [Gadgets and Gear](#)

Smartphones are all the rage in Army circles, as top generals talk up the prospect that only a few technical fixes stand in the way of a soldier having an iPhone or an Android phone as part of his basic kit. But don't expect the Army to scrap the suite of wearable computers, cameras, radios, GPS and digitized maps it's spent years developing just because a phone you can buy at Best Buy makes its functions redundant.

Like [a superhero designed by Rob Liefeld](#), that system, called Nett Warrior, snakes cables around a soldier's body armor to [network him with his unit or headquarters](#) through an array of computers and peripherals. It adds between 12 to 15 pounds to his load. But the biggest challenge to Nett Warrior comes from the phones soldiers carry in their pockets — when they're in civilian gear, that is.

"Every kid's going down to whatever local store they want and they're buying some smart device and saying, 'Well, this is modern, and it lets me know where I am, where my friends are ... it gives me all that capability, how come I can't get that?'" acknowledges Brig. Gen. Peter Fuller, the officer in charge of outfitting soldiers with all their standard gear, who oversees Nett Warrior. "We're trying to figure out: How do we move Nett Warrior from its current configuration?"

Fuller's shop, PEO Soldier, will send Nett Warrior — the son of an earlier, failed program called [Land Warrior](#) — into "full-rate production" around June. But to some in the Army, it already smacks of outdated technology. An Apps for the Army contest last year proved there are [amateur developers in the service](#), ready to design Army-relevant functions for the Apple Store or the Android Market.

Accordingly, defense companies are creating [apps of their own for tracking or mapping](#). Gen. Peter Chiarelli, the Army's vice chief of staff and an iPhone enthusiast,

Soldiers' Wearable Computers May Get an iPhone Brain

told Danger Room in February, “we can already see the [benefit for the squad and team leader](#)” of smartphones.

A program within the Army’s Training and Doctrine Command (TRADOC), called [Connecting Soldiers to Digital Applications](#), is running parallel to Nett Warrior in thinking through how iPhones and Droids can be most useful to the Army. The officer overseeing it, Lt. Gen. Michael Vane, told Military.com’s Christian Lowe point blank that “[smartphones could be the answer to the Nett Warrior requirement.](#)”

During a roundtable on Thursday with reporters at his Pentagon office, Fuller is sympathetic to a lot of that. Yes, smartphones are cool; yes, they’re a lot lighter than Nett Warrior; and no, they don’t have a ton of cables sticking out to entangle a soldier on dismounted patrol.

His solution: Marry the two together. Maybe take out the computer that serves as Nett Warrior’s brain “and give you a smart device” instead, he says when Danger Room asks him about smartphones and Nett Warrior’s future.

“We need a program to work from,” Fuller says, “and we’re saying Nett Warrior is that program. So get it through the milestone, and then you can make all the adjustments.”

The Army still has a way to go with smartphones, as TRADOC officers involved in the smartphone push have acknowledged to Danger Room. It has not decided whether it prefers the iPhone, Android phones or Windows phones. (The open architecture of the Droids might have an edge, though.)

It’s not sure how configure them for a low-bandwidth environment like, say, Afghanistan. And it has not yet figured out how to secure them, so an Android phone doesn’t “tell Google where we are all the time, because we’re tied to GoogleMaps,” as

Soldiers' Wearable Computers May Get an iPhone Brain

Fuller puts it. Darpa, it's worth noting, is [working on that last part](#).

Another unresolved question: Should the Army actually issue phones to soldiers, or give them requirements and an allowance, so they can buy their own phones and upgrade as necessary?

Until the Army resolves all that, it's going to be some time before smartphones are as much a part of the Army as the M4 rifle. The drawback is that it might spend millions on Nett Warrior as a stopgap measure that practically has to be replaced as soon as it's complete.

Fuller, who's leaving PEO soldier for a tour in Afghanistan, argues that the best way to getting smartphones into soldiers' pockets is to incorporate them into Nett Warrior. But he's up front about the frustrations of the program. "I tell people, we are at the one-yard line, in our red zone," he says. "And everyone's looking at the cheerleaders and going, 'Hey, I like what they got over on the sidelines.'"

Military Apps Putting iPhone in the Battlefield

Military apps putting iPhone in the battlefield

iPhone apps being developed for military mapping, surveillance

By Brad Reed, Network World
April 14, 2011 10:13 AM ET



While it's unlikely that future wars will be won or lost by [iPhone applications](#), it's entirely possible that [Apple smartphones](#) deployed in the battlefield could soon be saving lives.

That's because application developers such as Intelligent Software Solutions (ISS) and Harris Corp. are working to create military applications that soldiers can use to gather intelligence and map out dangerous areas in hostile territory. John DeLay, the director of strategy and architecture for Harris' small and medium business division, says that the addition of improved video capabilities on smartphones has made the iPhone and comparable devices legitimate surveillance tools that can capture high-quality images on the battlefield.

"As these hand-held devices have become more capable as collectors for video, they have become more attractive and useful in Department of Defense applications," he says. "We have a number of applications we're developing in the DoD space that would run on either [Android](#), iOS or the BlackBerry platform."

One such application is a military variation of Harris' Newsfish, which bills itself as a tool for "citizen journalists" who want to create videos and upload them onto blogs and news sites. DeLay says the military version of the app would allow soldiers to act as reporters and record videos with their smartphones that can be securely uploaded onto the military's enterprise architecture.

"The enterprise architecture has been designed to deal with all types of motion imagery, whether it comes from iPhones, Android devices, or Predator drones of Global Hawks," he says.

Another application Harris is developing is designed more for the [iPad](#) and other tablets that will let users remotely control fixed cameras and capture/edit footage in real time. DeLay says that the iPad is a good form factor for this particular app because it is more durable than a smartphone and because its larger screen will allow for "Madden-style telestration" where users can draw pictures

Military Apps Putting iPhone in the Battlefield

or make notes on live video feeds, similar to how football commentators draw on television screens during games.

Military mapping

The military application being designed by Intelligent Software Solutions, meanwhile, doesn't rely on video-shooting capabilities and instead is more of a mapping application that military personnel can use to report, collect and analyze data while in the theater of war. So for instance, soldiers using the application and GPS technology could mark down certain dangerous hot spots that have seen frequent insurgent attacks or are frequently targeted with improvised explosive devices. This data is then uploaded into a central database where it can be used to analyze where military personnel can roam freely and where they should proceed with extreme caution.

Rob Rogers, vice president of national systems at ISS, emphasizes that most military smartphone applications are still quite a ways from being deployed in the battlefield. Currently, he says that the military is mostly experimenting with the possibility of utilizing smartphones in theater and that most of the smartphones brought into battle are personal devices owned by soldiers.

"There are a lot of personally owned cellphones that people take with them, but it's just now starting to proliferate on an official level," he says. "The concept of a cellphone application is kind of new and there's always a lag in between when the public and the military starts to adopt some things."

And then, of course, there are issues with connectivity and [security](#), especially since places such as rural Afghanistan aren't exactly brimming with [3G networks](#) or network operations centers. DeLay notes that before any smartphones or tablets are deployed in theater they must be outfitted with proper encryption tools and the ability to hook onto whatever ad hoc [wireless](#) networks the military sets up.

"This is the reason we have a lot of work going on to have a [Type 1](#) encrypted iPad that will open up the ability to transmit data securely," he says. "So then in theater you'll be deploying secure 3G infrastructure, and you would then utilize the secure network to forward data to operation centers."

DoD to Rewrite Acquisition Requirements Process

DoD To Rewrite Acquisition Requirements Process

By DAVE MAJUMDAR

Published: 14 Apr 2011 14:19

COLORADO SPRINGS, Colo. - The U.S. Defense Department is scrapping the ponderously slow Joint Capabilities Integration and Development System (JCIDS) process, which defines acquisition requirements for the military.

"We're starting to rewrite JCIDS. We're going to throw it away," U.S. Marine Corps Gen. James Cartwright, vice chairman of the Joint Chiefs of Staff (JCS), said April 14 before an audience at the 27th National Space Symposium. "We're going to try to align ourselves with acquisition and three levels of risk."

Cartwright said the new strategy would allow the Defense Department to more quickly buy urgently needed equipment. Such systems could range from a truck to something the size of an aircraft carrier.

"It demands of industry to go out to get the tools that allow us to build a truck in less than 14 years," Cartwright said.

It would also allow the Defense Department to buy space systems for one-third of the cost it now pays because the Pentagon would be able to buy equipment off the shelf.

Related to the process, Cartwright said, "As we stand down Joint Forces Command, we will move that function into the J-7 of the Joint Staff. And we will align J-8 and J-7."

The J-8 will be material solutions, J-7 will be non-material solutions. The two offices will work together under auspices of the vice chairman of the JCS, he said.

Having the two offices under one roof is key, Cartwright told reporters after his speech.

"I want one person in charge of that, so they can oversee it," he said.

The two offices will ensure that if the Defense Department has to purchase hardware,

DoD to Rewrite Acquisition Requirements Process

all of the necessary training and ancillary hardware is available, Cartwright said.

He cited real-world absurdities, such as satellites being in orbit without the necessary ground terminals to use them, as situations the two offices would work to avoid.

Defense Pursues 15-year Satellite Lease to Cut Battlefield Communications Costs

Defense pursues 15-year satellite lease to cut battlefield communications costs

BY BOB BREWIN 04/14/2011

The Pentagon spends \$500 million a year on commercial satellite communications to support operations in Afghanistan and Iraq. The Defense Information Systems Agency wants to cut those costs dramatically with a \$440 million, 15-year lease of a single commercial satellite. DISA expects such a deal could meet 78 percent of U.S. Central Command's requirements.

CENTCOM forces also could tap into military satellite services from two low-bandwidth Defense Satellite Communications System satellites and a single high-capacity Wideband Global Satcom satellite in orbit over the Indian Ocean. But these satellites hardly keep up with growing demand, and commercial operators provide 80 percent of the CENTCOM satellite service today.

Bruce Bennett, DISA's director for satellite communications, said end users in Afghanistan demand and expect the same kind of broadband service available in the United States, "and the only way to do that is by satellite." Short-term leases of commercial capacity is costly, Bennett said, which is why DISA wants to explore a long-term lease option with commercial satellite operators.

Last month, DISA asked industry for its input on this lease deal -- Assured SATCOM Services in Single Theater. Industry responses to the request for information are due April 15. DISA asked satellite operators if they could provide broadband service during a 15-year period for \$440 million. The 2012 DISA budget request allocates \$86.7 million for the project in 2011 and \$415 million in 2012.

In the request for information, DISA said it wants to lease a single satellite to provide service in the commercial Ku-band as well as the Ka-band, which military Wideband Global Satcom satellites use.

DISA plans to use commercial Ku-band service to support remotely piloted aircraft operations and the Ka-band service for ground forces. The total throughput from the leased commercial satellite is pegged at 6.37 gigabits per second, or about the same capacity as the military Wideband Global Satcom satellite serving CENTCOM today.

Bennett said that while a Ku/Ka-band satellite that could meet DISA's requirements "does not exist today," his discussions with satellite operators indicated that one was under construction.

Britt Lewis, vice president of marketing and business strategy for Intelsat General Corp., said, "It is possible to build a satellite between now and December 2014 to fully meet the ASSIST requirements as long as the bidder has access to the relevant Ku-band spectrum," to support

Defense Pursues 15-year Satellite Lease to Cut Battlefield Communications Costs

operations for remotely piloted aircraft.

Rebecca Cowen-Hirsch, president of Inmarsat Government Services Inc., said it would be "impossible" for DISA to acquire a combined Ku/Ka-band satellite to serve CENTCOM by December 2014 as the agency plans. Cowen-Hirsch said commercial operators do not have either the satellites or the orbital slots to meet this requirement. She suggested DISA drop the Ku-band requirement and instead focus on acquisition of a Ka-band only satellite. Inmarsat will have such a satellite that can meet DISA's needs in 2013, she said.

DISA, in response to questions from satellite operators, said that while it wants to acquire Ka-band capacity on one satellite and prefers to obtain Ku-band service over the same satellite, "there is more flexibility in how the Ku capacity is provided."

The 2012 DISA budget for the CENTCOM commercial satellite service includes \$362.9 million for the long-term satellite lease and another \$53.1 million to upgrade terminals, replacing the Ku-band terminals remotely piloted aircraft use with Ka-band terminals. Cowen-Hirsch suggested DISA put more of this budget into terminal replacement, which would eliminate the need for Ku-band service.

Lewis said remotely piloted aircraft currently account for 20 percent of the CENTCOM satellite capacity, with those requirements expected to grow. "Our sense is that [unmanned aerial systems] demand will continue to escalate as long as the government continues its high operations tempo around the world," Lewis said.

Cowen-Hirsch said the DISA ASSIST program represents an intriguing and innovative opportunity for a public-private partnership that will help drive down satellite lease costs for Defense while providing satellite operators with a long-term customer.

DISA, in its budget request, said the long-term lease will provide it with 78 percent of the CENTCOM satellite capacity through an "efficient, economic and dedicated source."

US Navy Getting Closer to Arming Ships with Lasers

U.S. Navy getting closer to arming ships with lasers
by Christopher MacManus



The U.S. Navy's solid-state, high-energy laser.
(Credit: U.S. Navy photo by John F. Williams)

"Fire the laser!" may sound like something straight out of "Star Wars," but that phrase could one day be common on U.S. Navy ships.

Northrop Grumman and the Office of Naval Research recently concluded a series of [successful solid-state laser defense firing tests](#) aboard the decommissioned Spruance-class destroyer USS Paul F. Foster (a remotely driven self-defense test ship). The Maritime Laser Demonstrator zapped away at an assortment of objectives at the Pacific Ocean Test Range off the central California coast, including land-based targets and remotely driven small boats that traveled at various speeds.

It was the first time a laser of such strength had been fired from a moving ship at sea. This is also the first system to be integrated with a Navy ship's radar and navigation system, ensuring a much higher level of accuracy. The U.S. Navy collaborated with the Office of the Secretary of Defense's High Energy Joint Technology Office and the Army's Joint High Powered Solid State Laser program to bring this once-imagined weapon to life.

US Navy Getting Closer to Arming Ships with Lasers

"The results show that all critical technologies for an operational laser weapon system are mature enough to begin a formal weapon system development program," [Steve Hixson](#), vice president of space and directed energy systems at Northrop Grumman's Aerospace Systems sector, said in a statement. "Solid-state laser weapons are ready to transition to the fleet."

The next step is "the engineering, manufacturing, and development phase," according to Northrop Grumman. The Navy plans to outfit up to eight classes of ships in the fleet with this next-generation weapon, but these beams aren't quite ready to replace traditional weapons systems, according to Chief of Naval Research Rear Adm. Nevin Carr. Nevertheless, these lasers sure could cause a bad day for smaller craft.

In the video below, we see just exactly how little time it takes for a laser to melt away critical components on a small boat. After a few seconds of maintaining laser contact, a fire erupts in the engine, causing total loss of power on the rogue ship.

The Navy's Acquisitions Hiring Boom

The Navy's acquisitions hiring boom

By [Philip Ewing](#) Friday, April 15th, 2011 4:57 pm
Posted in [Naval](#)

The Navy's Department's top weapons-buyer, Sean Stackley, set down a priority this week at the Sea Air Space show that probably won't get a lot of attention like the "Great Green Fleet" or the "313-ship Navy." Still, he said he hopes it could pay huge dividends if successful. The department, Stackley said, needs to add thousands of uniformed and civilian acquisitions experts who know how to smooth out the complicated process of buying big, expensive things. Not as flashy as [a rail gun](#), but it could save the department hundreds of millions of dollars.

"Ten to 15 years of downsizing has thinned our professional corps and we need to reverse that decline," Stackley said. That includes deckplate-level inspectors working for the Supervisor of Shipbuilding, program managers, contract wranglers, test and evaluations professionals, and so on. For the past several years, the Navy has struggled with accepting warships that needed expensive re-work after entering the fleet, or which sailed late or over-budget because of quality problems. Just this week, you read here on Buzz about how [manufacturing problems caused hull cracks](#) aboard the littoral combat ship USS Freedom.

According to information provided Friday by Navy spokeswoman Capt. Cate Mueller, the goal is to increase the Navy's acquisition workforce across the board by about 16 percent, or more than 6,000 people, over the next five years. Most of those people will be government employees, either service members or full-time Navy Department workers.

"We're doing this at the expense of support contracts, but that's a good trade-off," Stackley said Wednesday. "The goal is not to restore government employees, but to restore our core competence."

US Products Help Block Mideast Web

U.S. Products Help Block Mideast Web

By [PAUL SONNE](#) And [STEVE STECKLOW](#)

As Middle East regimes try to stifle dissent by censoring the Internet, the U.S. faces an uncomfortable reality: American companies provide much of the technology used to block websites.

McAfee Inc., acquired last month by Intel Corp., has provided content-filtering software used by Internet-service providers in Bahrain, Saudi Arabia and Kuwait, according to interviews with buyers and a regional reseller. Blue Coat Systems Inc. of Sunnyvale, Calif., has sold hardware and technology in Bahrain, the United Arab Emirates and Qatar that has been used in conjunction with McAfee's Web-filtering software and sometimes to block websites on its own, according to interviews with people working at or with ISPs in the region.

CENSORSHIP INC.

A regulator in Bahrain, which uses McAfee's SmartFilter product, says the government is planning to switch soon to technology from U.S.-based Palo Alto Networks Inc. It promises to give Bahrain more blocking options and make it harder for people to circumvent censoring.

Netsweeper Inc. of Canada has landed deals in the UAE, Qatar and Yemen, according to a company document.

Websense Inc. of San Diego, Calif., has a policy that states it "does not sell to governments or Internet Service Providers (ISPs) that are engaged in government-imposed censorship." But it has sold its Web-filtering technology in Yemen, where it has been used to block online tools that let people disguise their identities from government monitors, according to Harvard

US Products Help Block Mideast Web

University and University of Toronto researchers.

Websense's general counsel said in a 2009 statement about the incident:

"On rare occasion things can slip through the cracks."

'Filtering' the Web in the Middle East and North Africa

Map shows nations that have used Western-made technology to block websites the governments deem objectionable. Screenshot, below, is what some citizens in the U.A.E. see when visiting a blocked site.



Some web addresses blocked as of this month:

BAHRAIN:	U.A.E:	YEMEN:
BahrainRights.org Website for Bahrain Center for Human Rights	Orkut.com Social networking site owned by Google	YemenPortal.net Aggregates news about Yemen
Malkiya.net News and forum site for village of Malkiya	Ahmedandsalim.com Animated web series parodying terrorists	Al-teef.com News and info site from Yemen

Web-filtering technology has roots in the 1990s, when U.S. companies, schools and libraries sought to prevent people from surfing porn, among other things.

Today, that U.S. technology is now among the tools used in the clampdowns on uprisings across the Middle East. In Egypt, Syria, Tunisia and elsewhere, bloggers have been jailed and even beaten as governments try to repress online expression.

In Bahrain, Nabeel Rajab, head of the banned Bahrain Human Rights

US Products Help Block Mideast Web

Center, which runs a website the government blocks, says he was briefly thrown in a car and roughed up after authorities raided his house last week. The men threatened him with a pipe, he says, and slapped him when he refused to say he loved Bahrain's king and prime minister.

For the U.S., the role of Western companies in Internet censorship poses a dilemma. In a speech last year, Secretary of State Hillary Rodham Clinton said, "Censorship should not be in any way accepted by any company from anywhere. And in America, American companies need to take a principled stand."

Lately the State Department has spent more than \$20 million to fund software and technologies that help people in the Middle East circumvent Internet censorship that is sustained by Western technology.

Asked about that policy, a senior State Department official said the U.S. is responding to "a problem caused by governments abusing U.S. products." When governments repurpose U.S.-made tools "to filter for political purposes, we are involved in producing and distributing software to get around those efforts."

A Bahrain official defended censorship. "The culture that we have in the Middle East is much more conservative than in the U.S.," says Ahmed Aldoseri, director of information and communication technologies at the Telecommunications Regulatory Authority.

Freedom of speech is guaranteed in Bahrain, Mr. Aldoseri says, "as long as it remains within general politeness."

Makers of Web-filtering technology say they can't control how customers use their products. "You can add additional websites to the block list," says Joris Evers, a McAfee spokesman. "Obviously what an individual customer would do with a product once they acquire it is beyond our control." A spokesman

US Products Help Block Mideast Web

for Blue Coat made similar points.

There are no special export restrictions on Web-filtering technology. Anti-censorship advocates say there needs to be a way for companies to track how their filtering software is used.

"They could build into the software something that signals and, in fact, sends back to them exactly what kind of filtering is taking place," says Jonathan Zittrain, a professor of law and computer science at Harvard Law School. "There's no rocket science there, it's just their customer wouldn't like it."

Web-blocking companies declined to name their Middle Eastern customers, but The Wall Street Journal identified a number of them through interviews with ISPs, a reseller and former employees. In addition, OpenNet Initiative, made up of Harvard and University of Toronto researchers who study Internet filtering, identified three ISPs in Yemen, Qatar and the UAE that were using Netsweeper in January. ISPs provide Internet access to households and companies.

Mideast Upheaval

A Netsweeper official said the company doesn't comment on its clients.

According to a forthcoming report from OpenNet, ISPs in at least nine Middle East and North African countries have used "Western-made tools for the purpose of blocking social and political content, effectively blocking a total of over 20 million Internet users from accessing such websites."

Employees at ISPs in the Middle East said in interviews that government ministries give them databases of Internet addresses, including, at times, antigovernment sites, for blocking and that they must comply. The number of requests varies by country.

Mishary Al-Faris, quality assurance manager at Qualitynet in Kuwait, says his ISP, which uses SmartFilter, receives several requests a year from the

US Products Help Block Mideast Web

government to block content deemed religiously offensive. "It's kind of a gentlemanly understanding: 'We're going to honor your requests,'" he says.

Web-filtering isn't exclusively a tool of Internet censorship. As companies like McAfee, Blue Coat and Netsweeper note, their technology can prevent youngsters from encountering pornography and protect ISPs from malicious cyber attacks.

In recent years, American companies aggressively have sought new customers abroad. The global Web-security market, including filtering, was valued at \$1.8 billion in 2010, according to Phil Hochmuth of market-research firm IDC. The Middle East and Africa accounted for about \$46 million and is growing at about 16% a year, he says.

China is considered the king of Web filtering, with its elaborate censorship system dubbed the "Great Firewall." China's technology remains unclear but its reach is vast: Local Chinese sites must be licensed and are required to remove any content the government deems objectionable. In addition, some major foreign sites, including Facebook, Twitter and Google Inc.'s YouTube, have been blocked for more than a year.

Middle East Web blocking has some differences. Government licenses for websites typically aren't required. Another difference: In the Middle East the ISP will generally show an explicit notice saying a site has been blocked, whereas in China it is often unclear why a site becomes inaccessible.

Blocking websites can be done with hardware, specialized software or a combination of the two. On a basic level, Web filtering works this way: First, a list is built that groups websites into categories such as "gambling," "dating" or "violence." Netsweeper says it has categorized more than 3.8 billion Web addresses and adds 15 million a day. Then, a user of the software can use that list to block access to specific sites or categories.

Companies like Websense and Netsweeper can now scan and categorize

US Products Help Block Mideast Web

the content of an uncategorized page in real time. They can also block pieces of a site, rather than whole pages, if only a certain image or text is considered objectionable.

The use of filtering to block websites could be seen this month in Bahrain, where a group of mostly Shia protesters took aim at the country's Sunni ruling family and met a violent crackdown. Batelco, Bahrain's main ISP, filters the Web using McAfee SmartFilter software and Blue Coat technology, according to Ali AbuRomman, who works on the network team. He says the government regularly uploads lists of websites to block, including some political sites, to the country's ISPs.

In a test on a Batelco connection in Bahrain in recent days, The Wall Street Journal found that online-community forums for Shia villages and the websites of at least two human-rights groups were censored.

"Site blocked," the screen read in English and Arabic when a Journal reporter tried to view the sites. "This website has been blocked for violating regulations and laws of Kingdom of Bahrain."

Since 2009, Bahrain has had the power to order the blocking of websites for "transgressing local values and impairing national unity," according to the U.S. State Department.

Also blocked during the Journal test was Malkiya.net, a news site and discussion forum for Malkiya, a mostly Shia fishing town that has seen antigovernment protests in recent years. Its owner, Ali Mansoor Abbas, says the site also was blocked after it covered protests over the seizure of part of a local beach by a cousin of Bahrain's king.

Mr. Aldoseri, the Bahrainian telecom official, says his country plans to switch in the next few months from SmartFilter to technology from Palo Alto Networks. It can block activities within websites, like video or photo uploading, or Internet tools that let users bypass blocking altogether, which

US Products Help Block Mideast Web

are illegal in Bahrain.

Middle East Web filtering has sparked a cat-and-mouse game to outfox the censors. Website owners like Mr. Abbas of Malkiya.net sometimes create "mirror" sites, with slightly different names.

Walid Al-Saqaf, a graduate student and former journalist from Yemen who now lives in Sweden, engineered his own circumvention tool after his news-aggregation site, YemenPortal.net, which included antigovernment content, was blocked by the country's filters. Known as Alkasir, the Arabic word for "circumventor," his free program has attracted at least 16,000 users in Yemen, China, Iran and elsewhere, he says.

Two years ago, OpenNet Initiative researchers found that Yemen was using filtering software from Websense to block privacy tools. In response, the company said it stopped providing the ISPs involved with its latest website-block lists since the ISPs violated its anticensorship policy.

The new OpenNet report says Websense tools and services appeared to still be used in Yemen as recently as August. The company declined to comment. The report also found that in January, new filtering software was being used in Yemen from Canadian firm Netsweeper.

"Filtering decisions are made by the entity that decides to filter," says Scott O'Neill, Netsweeper's director of sales and marketing. "Much as Ford Motor Co. can't decide how [its customers] are going to drive their cars."

An informational company document says telecom companies can use Netsweeper to "block inappropriate content using [a] pre-established list of 90+ categories to meet government rules and regulations—based on social, religious or political ideals."

Emirates Integrated Telecommunications Co., or Du, one of the UAE's main ISPs, decided last year to switch to Netsweeper from the filtering system it

US Products Help Block Mideast Web

had been using with Blue Coat devices, says Abul Hasan Jafery, a technical consultant who helped implement Netsweeper's filtering system there.

"We block malware, alternative lifestyles, profanity," says Mr. Jafery. "If something is offensive to the religion, we block it."

Until recently, Tunisia had some of the most pervasive Internet filtering in the world, according to OpenNet. Then, a January popular revolt forced the resignation of the country's president—triggering the wave of protests that have spread across the Middle East.

Tunisia has since pulled the plug on its Web-blocking gear. The new head of the Tunisian Internet Agency, Moez Chakchouk, says he was astounded when he recently visited a secured room at the state telephone company where the filtering equipment was kept.

The room was full of unfamiliar gear, says the 36-year-old computer engineer, who took the job last month. "I don't know" what it all does, he says. Mr. Chakchouk says the Interior Ministry controlled the filtering equipment since 2004, and the entire country's Internet traffic flowed through it.

For several years, according to Mr. Chakchouk, the Tunisian government used SmartFilter, which McAfee acquired in 2008. The McAfee spokesman confirmed the product has been sold in Tunisia, but declined to disclose its customers.

For better or worse, says Mr. Chakchouk, part of the legacy of Tunisia's former regime has been to leave Tunisia with some of the most sophisticated Internet-filtering equipment in the world. "I had a group of international experts from a group here lately, who looked at the equipment and said: 'The Chinese could come here and learn from you.'"

—Marc Champion, Christopher Rhoads, Nicholas Casey and Loretta Chao contributed to this article.

Engineering vs. Liberal Arts: Who's Right—Bill or Steve?

Engineering vs. Liberal Arts: Who's Right—Bill or Steve?

Vivek Wadhwa

Mar 21, 2011



When students asked what subjects they should major in to become a tech entrepreneur, I used to say engineering, mathematics, and science—because an education in these fields is the prerequisite for innovation, and because engineers make the best entrepreneurs.

That was several years ago.

I realized how much my views have changed when the The New York Times asked me to write a piece for its “Room for Debate” forum this week. The paper wanted me to comment on the divergence of opinion between Bill Gates and Steve Jobs. In a **speech** before the National Governors Association on Feb 28, Gates had argued that we need to spend our limited education budget on disciplines that produce the most jobs. He implied that we should reduce our investment in the liberal arts because liberal-arts degrees don’t correlate well with job creation. Three days later, at the unveiling of the iPad 2, Steve Jobs said: “It’s in Apple’s DNA that technology alone is not enough—it’s technology married with liberal arts, married with the humanities, that yields us the result that makes our heart sing, and nowhere is that more true than in these post-PC

Engineering vs. Liberal Arts: Who's Right--Bill or Steve?

devices”.

Because I am a professor at the Pratt School of Engineering at Duke University, and given all the **positive things I say** about U.S. engineering education, The Times assumed that I would side with Bill Gates; that I would write a piece that endorsed his views. But, even though I believe that engineering is one of the most important professions, I have learned that the liberal arts are equally important. It takes artists, musicians, and psychologists working side by side with engineers to build products as elegant as the iPad. And anyone—with education in any field—can achieve success in Silicon Valley.

Here is what I wrote for The Times.

It's commonly believed that engineers dominate Silicon Valley and that there is a correlation between the capacity for innovation and an education in mathematics and the sciences. Both assumptions are false.

My research team at Duke and Harvard **surveyed** 652 U.S.-born chief executive officers and heads of product engineering at 502 technology companies. We found that they tended to be highly educated: 92 percent held bachelor's degrees, and 47 percent held higher degrees. But only 37 percent held degrees in engineering or computer technology, and just two percent held them in mathematics. The rest have degrees in fields as diverse as business, accounting, finance, health care, and arts and the humanities.

Gaining a degree made a big difference in the sales and employment of the company that a founder started. But the field that the degree was in and the school that it was obtained from were not a significant factor.

Over the past year, I have interviewed the founders of more than 200 Silicon Valley start-ups. The most common traits I have observed are a passion to change the world and the confidence to defy the odds and succeed.

It is the same in business. In the two companies I founded, I was involved in

Engineering vs. Liberal Arts: Who's Right--Bill or Steve?

hiring more than 1000 workers over the years. I never observed a correlation between the school of graduation or field of study, on one hand, and success in the workplace, on the other. What make people successful are their motivation, drive, and ability to learn from mistakes, and how hard they work.

And then there is the matter of design. Steve Jobs taught the world that good engineering is important but that what matters the most is good design. You can teach artists how to use software and graphics tools, but it's much harder to turn engineers into artists.

Our society needs liberal-arts majors as much as it does engineers and scientists.

But I need to acknowledge the difficult reality: that employment prospects are dim for liberal-arts majors. Graduates from top engineering schools such as Duke are always in high demand. But PhDs in English from even the most prestigious universities, such as UC-Berkeley, **can't get jobs**. The data I presented above were on the background of tech-company founders—those who made the transition into entrepreneurship. Most don't. And, as you can note from Bill Gates' speech, there is a bias against liberal arts and humanities.

Angelika Blendstrup is an author and a lecturer who holds a PhD in Bilingual Bicultural Education from Stanford. She says that her liberal-arts background is “great for writing papers or PhDs, but it would be better to have studied engineering and have a choice of jobs”.

Charles River Venture Partner emeritus, Ted Dintersmith, on the other hand, received a PhD in Engineering from Stanford. But he also studied liberal arts. Ted says “It doesn't have to be either/or—I double-majored in Physics and English, and never regretted combining two such different disciplines”.

So there is no black and white here. We need musicians, artists, and psychologists, as much as we need bio-medical engineers, computer

Engineering vs. Liberal Arts: Who's Right--Bill or Steve?

programmers, and scientists.

My advice to my students—and to my own children—is to study what interests them the most; to excel in fields in which they have the most passion and ability; to change the world in their own way and on their own terms. Once they master their domain, they can find the path to entrepreneurship. They can then come up with creative ways of solving the problems that they have encountered, and apply their ideas to other fields where their knowledge adds value. Maybe they can team up with the hard-core engineers who develop the clunky, inelegant, over-engineered products that Bill is famous for; maybe work with Steve to create the next iPhone or iPad.

Editor's note: **Vivek Wadhwa** is an entrepreneur turned academic. He is a Visiting Scholar at UC-Berkeley, Senior Research Associate at Harvard Law School, Director of Research at the Center for Entrepreneurship and Research Commercialization at Duke University, and Distinguished Visiting Scholar at The Halle Institute for Global Learning at Emory University. You can follow him on Twitter at [@vwadhwa](https://twitter.com/vwadhwa) and find his research at www.wadhwa.com.

A Model for the Big Data Era

A Model For The Big Data Era

Data-centric architecture is becoming fashionable again By Rajive Joshi

By **Rajive Joshi** [InformationWeek](#)

March 26, 2011 12:00 AM

Wired and wireless communication networks are making data collection and transmission cheap and widespread. In the future, networks will weave many devices and subsystems into complex integrated distributed systems that will become the fabric of business and daily life.

Building such distributed systems is far from simple; they must be assembled from independently developed software components. Integration, especially combined with real-time performance demands, becomes the key challenge.

This article outlines fundamental design principles that enable integration of distributed systems from components. I use a data-centric approach to this design, as the data is the key element that must flow through the various systems.

The key to data-centric design is to separate data from behavior. The data and data-transfer contracts then become the primary organizing constructs. With carefully controlled data relationships and timing, the system can then be built from independent components with loosely coupled behaviors. Data changes drive the interactions between components, not vice versa as in traditional or object-oriented design.

The resulting loosely coupled software components with data-centric interfaces are then integrated into a working system through a data bus. The data bus connects data producers to consumers and enforces the associated quality-of-service (QoS) contracts on the data transfers. This design technique is naturally supported by the Data Distribution Service (DDS) specification (informationweek.com/1295/ddj/spec) for real-time systems, which is a standard from the Object Management Group (omgwiki.org/dds). Implementations of this standard are available from many vendors.

The techniques described here are proven in hundreds of mission-critical applications including robotics, unmanned vehicles, medical devices, transportation, combat systems, finance, and simulation.

A Model for the Big Data Era

A Future Distributed System

To understand the dynamic nature of next-generation distributed systems, it helps to examine a representative scenario: an air traffic control system. Air traffic control in the future will integrate a variety of disparate systems into a seamless whole--a system of systems. On the edge is a real-time avionics system inside the aircraft. The control tower in the center communicates with the avionics system, and then out to data servers at the airport. The system thus comprises connectivity from the "edge" (devices) to the "enterprise" (infrastructure services).

The data in the avionics system flows at high rates and is time-critical. Violating timing constraints could result in the failure of the aircraft or jeopardize safety. Although aircrafts traditionally operate as independent units, future aircraft must integrate closely with automated traffic control and ground systems.

The control tower is another independent real-time system. It monitors various aircraft in the region, coordinates their traffic flow and generates alarms to highlight unusual conditions. The data is time-sensitive for proper local and wide area system operation. However, the system may have greater tolerance for delays than the avionics systems.

The control tower communicates with the airport's enterprise information systems, which track flight status and other data and may communicate with multiple control towers and other enterprise information systems. It also must synthesize passenger, flight arrival, and departure status information. Because it isn't in the time-critical path, the enterprise information system can be more tolerant of delays.

Key Design Challenges

This so-called "system of systems" must deal with a many issues, such as correctly handling myriad differences in data exchange, performance, and real-time requirements. The architecture also involves different technology stacks, design models, and component life cycles.

To support system growth and evolution, the integration must be robust enough to handle changes on either side of an interface. To do this, only minimal assumptions

A Model for the Big Data Era

should be made about the interfaces between systems--the interface specifications should describe only the invariants in the interaction. Behavior can then be implemented independently by each system; the interface between them shouldn't include any component-specific state or behavior. This avoids tight coupling.

The systems on either side of an interface may differ in quantitative aspects of their behavior, including different data volumes, rates, and real-time constraints. The term "impedance mismatch" is shorthand for all the nonfunctional differences in the information exchange between two systems. Critically, a developer can capture these nonfunctional aspects of the information exchange by attaching QoS attributes to the data transfer. With explicit QoS terms, responses to impedance mismatches can be automated, monitored, and governed.

Principles Of Data-Centric Design

Data-centric design recognizes that the essential invariant is the information exchange between systems or components. It describes the exchange in terms of a "data model" and data producers and consumers of the data, and it relies on four basic principles:

1. Expose the data and metadata. Data-centric design exposes the data and metadata as first-class citizens, and uses them as the primary means of interconnecting heterogeneous systems. Data is the primary means of describing the world as it is, independent of any component-specific behavior. Metadata refers to information about the data's layout and structure. A data-centric interface is defined by the metadata, which must contain all of the information required to encode and decode the data in a given format.
2. Hide the behavior. Data-centric design hides any direct references to operations or code of the component interfaces. An interface can't embed any component-specific state or behavior. Components implement behaviors that can change the data or respond to changes in data (the "world model").
3. Delegate data handling to a data bus. Separation of data handling and application logic is necessary for loosely coupled systems. The component application logic should focus on manipulating interface data, not managing and distributing it. The data bus is responsible for data handling and is the authoritative source of the world model

A Model for the Big Data Era

shared amongst the components.

4. Explicitly define data-handling contracts. These contracts should be specified by the application at design time, and enforced by the data bus at runtime. Delivery contracts specify the QoS attributes on data produced and consumed by a component, including timing, reliability, durability, etc. The data bus examines these "contracts," and if compatible, establishes data flows. The data bus then enforces QoS contracts, thereby providing the application code clear, known expectations.

In contrast, traditional messaging designs focus on functional or operational interfaces and overlook impedance problems. The interface QoS and timing aren't modeled, so all the interface state and communications issues are implicitly assumed. The result: a brittle, tightly coupled design. Adding components or interactions violates the assumptions, forcing system designers to rework the interfaces. The architecture becomes very hard to maintain and evolve.

Data-Centric Interfaces

A data-centric interface specifies the common, logically shared data model produced and consumed by a component, along with the QoS requirements.

A component can be seen as plugging into a software data bus via the data-centric interface that defines data inputs and outputs. When multiple components are present, the result is an information-driven, data-centric architecture in which data updates drive interactions between loosely coupled components.

A data-centric architecture reduces the integration problem since a component only has to integrate with the common data model intrinsic to the problem domain. Components implement data-centric interfaces that declare what they produce or consume. The QoS contracts ensure timing, reliability, and other requirements are met for any component, new or old. Thus, the system can grow and evolve.

The Data Bus

From a component programmer's perspective, the application code simply consumes and produces logically shared input and output variables on the data bus. Responsibility for data routing, delivery, and managing QoS is decoupled from the

A Model for the Big Data Era

application logic and delegated to the implementation of the data bus.

The data bus requirements are fulfilled naturally by software that conforms with the DDS specification. That document defines the data-centric, publish-subscribe communication model for building distributed systems.

Several implementations of the DDS standard are available today, including an open source implementation and several commercial versions from RTI, Gallium, and Milsoft, among others. Leading DDS implementations provide deterministic low-latency, high-throughput messaging and data caching. While the most natural fit for these products has been in industrial, avionic, and military applications, they also have long been used in financial services, where the rapid distribution and processing of data is critical. And increasingly, as companies must handle large volumes of data, these products are entering business IT organizations.

One of the principal benefits for businesses is that a data-centric architecture paves the way for the use of generic infrastructure components. These include databases, complex event processing modules, and Web services. These components plug into the bus without the need for extensive custom coding to integrate them into the computing infrastructure. Done right, this model makes it possible for a spreadsheet to automatically populate cells from data items it subscribes to from a larger data fabric. Because data-centric architectures have no direct coupling among the application component interfaces, components in the DDS model can be added and removed in a modular and scalable manner, letting companies add producers and consumers of data without a jump in complexity. As data volume expands, the simplicity of this architecture is likely to become a crucial part of a business's ability to keep up.

Rajive Joshi has worked in high-performance real-time distributed systems for more than 18 years, including implementing distributed messaging and data distribution caching infrastructure. Write to us at iwletters@techweb.com.

Microsoft Scheme Sniffs Out Unused Wireless Spectrum

Microsoft scheme sniffs out unused wireless spectrum

Volunteered equipment would map white spaces that unlicensed devices could use

By [Tim Greene](#), Network World
March 25, 2011 10:26 AM ET

[Microsoft](#) researchers have designed a scheme for measuring whether licensed radio frequencies are actually being used so [unlicensed devices can use it](#), something that may become necessary as demand for [wireless applications](#) grows.

The architecture, called SpecNet, would sense and map where spectrum is being used and more particularly where it's not -- so-called [white spaces](#), according to a paper being presented next week at the USENIX Symposium on Networked Systems Design and Implementation in Cambridge, Mass.

The problem faced by potential users of wireless devices is that much of the radio spectrum is licensed, which gives the license holders all rights to bands of spectrum whether they use it all or not. This potentially inefficient use of a limited resource could be improved if areas where license holders aren't using their frequencies can be detected and used on the fly by others who need to send and receive wireless traffic.

"Opportunistic spectrum access (OSA) is now increasingly seen as a necessity to meet the growing demands of wireless applications," the researchers say in the paper, "SpecNet: Spectrum Sensing Sans Frontières."

This available spectrum would be detected by a network of spectrum analyzers driven by local servers that are overseen by a master [server](#) which would push analysis tasks to the local servers, according to the research team.

So if an entity needed bandwidth in a given area, it could query SpecNet and find out what frequencies are available, says the team led by Microsoft researcher Anand Padmanabha Iyer. The network could measure available spectrum remotely and estimate the area covered by the primary transmitter of individual frequencies in particular areas.

One major hurdle to clear: the cost of the analyzers, which go for \$10,000 to \$40,000 each. The researchers suggest that the network be set up by volunteers who have spectrum analyzers to commit to SpecNet for assigned time periods. Each analyzer would be connected to a server that would issue commands to it via XML remote procedure calls over HTTP, making it possible to reach the machines over the Internet using whatever language they choose, they say. These servers

Microsoft Scheme Sniffs Out Unused Wireless Spectrum

would be networked to a command server that would oversee data collection over the network.

While use of white spaces has been approved in the U.S. by the FCC, no other country has given the OK to OSA. And studies of spectrum use have only been conducted in a handful of developed nations. SpecNet, with its use of equipment that is lent to the project, could broaden the studies and push other countries to approve OSA, the researchers say.

In the paper, the researchers work out the details of making the spectrum scans as quick as possible and sharing data collection among spectrum analyzers to keep the burdens on individual analyzers as light as possible.

In addition to discovering where white-space frequencies are available, the network could be used by enforcement agencies to pinpoint where individual transmitters are located so they can shut down individuals trying to use OSA illegally.

Success of SpecNet will rely on the good will and motivation of participants who would have to commit their equipment to the project. Participation might also require moving the location of the antennas for the spectrum analyzers, which are typically located in research facilities, often below ground level where signals are weaker, the researchers say.

Companies Hope to 'Program' the Internet

Thursday, March 31, 2011

Companies Hope to 'Program' the Internet

The Open Network Foundation wants to let programmers take control of computer networks.

By Kate Greene

Most data networks could be faster, more energy efficient, and more secure. But network hardware—switches, routers, and other devices—is essentially locked down, meaning network operators can't change the way they function. Software called OpenFlow, developed at Stanford University and the University of California, Berkeley, has opened some network hardware, allowing researchers to reprogram devices to perform new tricks.

Now 23 companies, including Google, Facebook, Cisco, and Verizon, have formed the Open Networking Foundation (ONF) with the intention of making open and programmable networks mainstream. The foundation aims to put OpenFlow and similar software into more hardware, establish standards that let different devices communicate, and let programmers write software for networks as they would for computers or smart phones.

"I think this is a true opportunity to take the Internet to a new level where applications are connected directly to the network," says Paul McNab, vice president of data center switching and services at Cisco.

Computer networks may not be as tangible as phones or computers, but they're crucial: cable television, Wi-Fi, mobile phones, Internet hosting, Web search, corporate e-mail, and banking all rely on the smooth operation of such networks. Applications that run on the type of programmable networks that the ONF envisions could stream HD video more smoothly, provide more reliable cellular service, reduce energy consumption in data centers, or even remotely clean computers of viruses.

The problem with today's networks, explains [Nick McKeown](#), a professor of electrical engineering and computer sciences at Stanford who helped develop OpenFlow, is that data flows through them inefficiently. As data travels through a standard network, its path is determined by the switches it passes through, says McKeown. "It's a little bit like a navigation system [in a car] trying to figure out what the map looks like at the same

Companies Hope to 'Program' the Internet

time it's trying to find you directions," McKeown explains.

With a programmable network, he says, software can collect information about the network as a whole, so data travels more efficiently. A more complete view of a network, explains Scott Shenker, professor of electrical engineering and computer science at the University of California, Berkeley, is a product of two things: the first is OpenFlow firmware (software embedded in hardware) that taps into the switches and routers to read the state of the hardware and to direct traffic; the second is a network operating system that creates a network map and chooses the most efficient route.

OpenFlow and a network operating system "provide a consistent view of the network and do that at once for many applications," says McKeown. "It becomes trivial to find new paths."

Some OpenFlow research projects require just a couple hundred lines of code to completely change the data traffic patterns in a network—with dramatic results. In one project, McKeown says, researchers reduced a data center's energy consumption by 60 percent simply by rerouting network traffic within the center and turning off switches when they weren't in use.

This sort of research has caught the attention of big companies, and is one reason why the ONF was formed. Google is interested in speeding up the networks that connect its data centers. These data centers generally communicate through specified paths, but if a route fails, traffic needs to be rerouted, says Urs Hoelzle, senior vice president of operations at Google. Using standard routing instructions, this process can take 20 minutes. If Google had more control over how the data flowed, it could reroute within seconds, Hoelzle says.

Cisco, a company that builds the hardware that routes much of the data on the Internet, sees ONF as a way to help customers build better Internet services. Facebook, for example, relies on Cisco hardware to serve up status updates, messages, pictures, and video to hundreds of millions of people worldwide. "You can imagine the flood of data," says McNab.

Future ONF standards could let people program a network to get different kinds of performance when needed, says McNab. Building that sort of functionality into Cisco hardware could make it more appealing to Internet services that need to be fast.

The first goal of the ONF is to take over the specifications of OpenFlow, says McKeown. As a research project, OpenFlow has found success on more than a dozen

Companies Hope to 'Program' the Internet

campuses, but it needs to be modified so it can work well at various companies. The next step is to develop easy-to-use interfaces that let people program networks just as they would program a computer or smart phone. "This is a very big step for the ONF," he says, because it could increase the adoption of standards and speed up innovation for network applications. He says the process could take two years.

In the meantime, companies including Google, Cisco, and others will test open networking protocols on their internal networks—in essence, they'll be testing out a completely new kind of Internet.

Microsoft, Google Spar Over Security Certification

April 11, 2011 10:44 AM PDT

Microsoft, Google spar over security certification

by [Jay Greene](#)

Microsoft today continued its cat fight with Google, calling out the company for apparently misleading customers about the security of its applications.

The software giant alleges that Google Apps for Government doesn't meet the level of security that **Google claims**. In a **blog post**, Microsoft's corporate vice president and deputy general counsel, David Howard, said that Google's Web-based productivity suite for government clients is not certified under the Federal Information Security Management Act.

That's important because federal agencies, which are huge clients of both Microsoft and Google, buy technology based, in part, on whether it has FISMA certification. That certification demonstrates the technology is secure enough for federal business. In fact, the suit in which the FISMA revelations were unearthed was filed by Google over the Interior Department's decision to award Microsoft a contract to provide Web-based e-mail. That agency employs 88,000 workers.

The filing, unsealed on Friday, is a Justice Department brief in the case. "On December 16, 2010," the government says, "counsel for the government learned that, notwithstanding Google's representations to the public at large, its counsel, the GAO and this court, it appears that Google's Google Apps for Government does not have FISMA certification."

That would seem to run counter to Google's claims that its applications do have FISMA certification. On a **site marketing its business software**, the company writes "Google Apps for Government, now with FISMA certification." And the company goes on to explain the significance of the certification: "Obtaining Federal Information Security Management Act (FISMA) certification & accreditation for Google Apps is critical to our US federal government customers, who must comply with FISMA by law."

Microsoft, Google Spar Over Security Certification

Google, though, says it's Microsoft that's off-base. It's received FISMA certification for Google Apps Premium. And Google Apps for Government is a version of that product with even better security, the company said.

"We did not mislead the court or our customers," David Mihalchik, an executive on Google's enterprise team, said in a statement. "Google Apps received a FISMA security authorization from the General Services Administration in July 2010. Google Apps for Government is the same system with enhanced security controls that go beyond FISMA requirements."

And Mihalchik notes that Microsoft's competing Business Productivity Online Suite, which won the Interior Department contract that triggered its suit, isn't FISMA certified.

Google may have a tough time convincing the court, though, according to Laura Taylor, the chief executive and founder of Relevant Technology, which specializes in security audits of financial institutions. She's the author of *The FISMA Certification & Accreditation Handbook*. Taylor says the General Services Administration, which issues so-called "authority to operate" letters under FISMA, are sticklers about even modest product changes. "They're pretty picky people," Taylor said.

When companies modify products, the GSA often wants them to seek new authorization, she said. Google, meanwhile, is merely trying to update its current FISMA certification to apply to Google Apps for Government. "My guess is that Google isn't going to win this," Taylor said.

The he said-she said claims are part of Microsoft's ongoing battles with Google, where it's challenged everything from Google's plans to buy travel data provider ITA software--a deal that **regulators approved with conditions** Friday--to the level of access to data it provides search

Microsoft, Google Spar Over Security Certification

rivals with in Europe, which led [Microsoft to file a complaint](#) with European regulators last month.

In this skirmish, Microsoft calls Google's integrity into question. "The Department of Justice has concluded squarely that Google Apps for Government does not have FISMA certification," Howard writes. "Open competition should involve accurate competition. It's time for Google to stop telling governments something that is not true."

Navy UCLASS Program to Develop Carrier-Based Unmanned Aircraft with Surveillance and Strike Capability by 2018

Navy UCLASS Program To Develop Carrier-Based Unmanned Aircraft With Surveillance And Strike Capability By 2018

(MILITARY & AEROSPACE ELECTRONICS 29 MAR 11) ... John Keller

PATUXENT RIVER NAS, Md. - The U.S. Navy is kicking off a program to develop a carrier-based unmanned aerial vehicle (UAV) by 2018 with the ability to carry out intelligence, surveillance, and reconnaissance (ISR) missions, as well as light attack missions, to support carrier air wing operations.

The U.S. Naval Air Systems Command at Patuxent River Naval Air Station, Md., on Monday issued a broad agency announcement (N00019-11-R-0031) for the Unmanned Carrier-Launched Airborne Surveillance and Strike (UCLASS) program, which will capitalize on existing military systems to launch, recover, and control unmanned aircraft, transfer data in support of time-critical strike operations, and conduct persistence ISR operations.

UCLASS will provide an unmanned aircraft capable of persistent surveillance and precision strike, and will represent a major step toward combining manned and unmanned aircraft operations aboard Navy aircraft carriers. The new unmanned surveillance and strike aircraft will become part of the traditional aircraft carrier air wing. A UCLASS detachment may operate independently or as part of an existing unit, be sustainable aboard the aircraft carrier, be maintained by fleet sailors.

The Navy has been experimenting with carrier-based unmanned strike aircraft, such as the Northrop Grumman X-47B unmanned combat air vehicle (UCAV).

The UCLASS system will be interoperable for joint forces at levels 1 to 4 per STANAG 4586, and have the capability to transfer control of the aircraft, sensors, and weapons among operators at U.S. military sea and land-based facilities. The system will use secure, jam-resistant line-of-sight and beyond-line-of-sight communications to transfer information and receive control instructions.

The UCLASS system will consist of the air vehicle, mission system, and a remote vehicle control system; a control segment that connects to external U.S. military and carrier air wing assets, Navy and U.S. military networks and satellite systems, and existing U.S. military tasking, collection, processing, exploitation, and dissemination; an aircraft carrier launch and recovery system, and a systems support.

The UCLASS aircraft avionics will include infrared and other electro-optical sensors, as well as radar and radio communications that are compatible with other carrier air wing systems.

The first part of the UCLASS program involves a study of alternative designs, concepts of operations, and systems requirements. Companies interested must respond to the Navy quickly. To be considered, companies must submit offers no later than 29 April 2011 -- one month away.

Military's Newest Recruit: C-3PO

Military's Newest Recruit: C-3PO

- By [Adam Rawsley](#)  April 5, 2011 | 1:30 pm | Categories: [DarpaWatch](#)

The Pentagon has spent decades and gazillions of dollars trying to build the perfect translation device. Now, its far-out research arm is looking at a new direction: a robot that can interpret all sorts of languages — *and* think for itself. That's right: The Defense Department wants to build a real-life version of C-3PO.

Thursday, Darpa announced its new [Broad Operational Language Translation, or BOLT](#), research initiative — the latest in a long, long line of military interpretation gadgets and algorithms. The United States tends to fight its wars in places where it [doesn't really speak the language](#). Training up troops in critical languages like Arabic would be difficult, time-consuming and not entirely practical on a large scale.

Enter BOLT, which Darpa has asked Congress to fund at [\\$15 million this year](#). Once developed, BOLT would act something like C-3PO from the *Star Wars* movies, performing a variety of difficult translation feats for troops in hostile territory.

It would go well beyond the array of handheld phrase-translation machines currently in use. BOLT would use language as well as visual and tactile inputs so that it can “hypothesize and perform automated reasoning in the acquired language.” The end result, Darpa's announcement says, will be a robot with visual and tactile sensors that can recognize 250 different objects “and understand the consequences (pre-state and post-state) of 100 actions, so that it can execute complex commands.”

The bot should be able to conduct both human-to-machine and human-to-human translation. On the human-to-machine end, Darpa wants BOLT to be able to understand human speech in English and one Arabic dialect, such that it can take “complex commands to control a desk-top application” like e-mail or Microsoft Excel.

For person-to-person translation, BOLT is intended to enable “multiturn, bilingual

Military's Newest Recruit: C-3PO

human-human conversation” between English and Arabic with a success rate of 90 percent. The translation would be “genre-independent,” meaning translation of language (either Mandarin or an Arabic dialect) regardless of whether it’s in a text message or just plain conversation.

The U.S. military has tried out all sorts of translation gizmos on the battlefield. But devices like the [Phraselator](#) and the Voice Response Translator are limited.

They can’t translate just any words you’d like to say. Instead, they spit out a few key phrases and words in local languages likely to be useful on the battlefield.

The blunt phrase exchanges can’t produce the kind of complex communication that the Defense Department would like soldiers to be able to engage in. They can also be [downright awkward](#) sometimes.

That’s why Darpa’s currently putting money into more sophisticated devices like BOLT and another Threepio-like translators. The agency asked Congress to fund its [Robotic Automatic Translation of Speech, or RATS](#), program at \$21 million this year, up from \$9 million in 2010.

RATS is supposed to be able to pull speech out of “noisy or degraded signals” and identify the language spoken. It’s also intended to sniff out not just the language spoken, but the person behind it, by using voice recognition technology to check the person against a most-wanted list.

Whatever comes of Darpa’s attempt to turn BOLT into a military C-3PO, let’s just hope the Pentagon doesn’t give it the continuously piqued accent of Anthony Daniels, the dude who played the protocol droid in the movies.

Military's Newest Recruit: C-3PO

It's annoying enough in English. It might be worse to hear it in Arabic.

Navy Wants Unmanned 'Doc-Bots'

Navy Wants Doc-Bots, Robo-Ambulances

- By [Adam Rawnsley](#)  April 6, 2011 | 5:34 pm | Categories: [Drones](#)

Not all of the military's robot research goes into creating unfeeling killing machines. Some of them are here to heal, like the Navy's plan to create a medical robot to treat troops carried by drones.

The Office of Naval Research recently announced that it's looking to build a prototype medical robot it calls the [Autonomous Critical Care System](#). ACCS' first job would be monitoring critical patients' vital signs. Eventually, though, the Navy wants its bot to provide fluid, drugs, anaesthesia, suction, oxygen and help regulate a patient's temperature.

The Navy envisions its medic-bot actually diagnosing and managing a number of "medically complex, life-threatening clinical events" for more than six hours — to be done either autonomously or with the assistance of a human caregiver. To do some of that critical management, ACCS would come equipped with its own drug kit, including "epinephrine, phenylephrine, dopamine, vasopressin, paralytics" among others.

Both the military and civilian sectors have been looking into [robotic medical care](#) for a while. Darpa, the military's bleeding edge technologists, recently teamed up with the National Institutes of Health (NIH) for research into "[robotic applications to surgery](#)," as well as "computerized therapist personalities."

The ACCS will be a tiny little bot. The Navy wants it to be 30 pounds, max, and should be able to fit into helicopters easily.

But the Navy doesn't just want a robo-doc. It's also looking for an unmanned ambulance — one that flies, preferably. The Office of Naval Research says it expects that "unmanned ground or air vehicles" will be available to carry wounded troops or disaster victims in the future and that their medic-bot will "validate effective patient

Navy Wants Unmanned 'Doc-Bots'

monitoring and control” on them while in transit.

It's not that far-fetched of an idea. The Israelis have been working on a [robotic ambulance](#) for years. In this country, prototype cargo-carrying drones are already a reality. In the air, there's the [K-MAX helicopter](#) drone which can carry 6,000 pounds and on the ground there's [BigDog, the robotic pack mule](#) able to haul up to 300 pounds. The Air Force and Marine Corps already are working getting their own airborne cargo drones and the Navy wants to build software that would allow the cargo-bots to [ferry the wounded by voice command](#), without the aid of pilots.

DARPA's Hologram Goggles Will Unleash Drone Hell

Darpa's Hologram Goggles Will Unleash Drone Hell

• By [Noah Shachtman](#)  April 11, 2011 | 7:00 am | Categories: [Air Force](#)



The Pentagon's mad-science arm wants robotic death-from-above, on demand. And the key to getting it done just might be holograms.

Let me explain. Right now, authorizing and targeting air strikes is a process that's sometimes bureaucratic, and sometimes dangerous as hell. Bureaucratic as in the [Stanley McChrystal phase of the Afghanistan war](#), when it took a gaggle of [lawyers, intelligence analysts, air controllers, and commanders](#) at multiple layers to put steel on target.

The result was fewer civilian casualties — but more U.S. troops, locked in firefights without air support. Dangerous as hell as in the Libya war, where NATO jets are accidentally offing Libyan rebels with such alarming regularity that the opposition forces are now [painting their vehicles' roofs pink](#), to distinguish them from Gadhafi's rides.

DARPA's Hologram Goggles Will Unleash Drone Hell

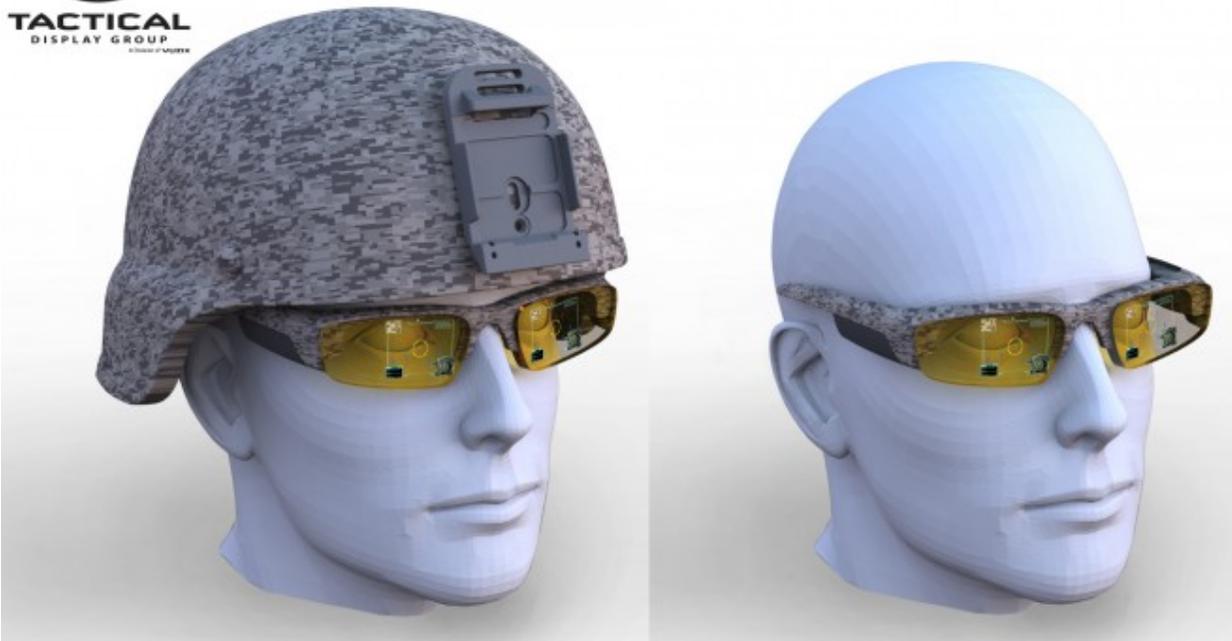
Darpa believes there might be a single technological fix to both problems: Give a single guy on the ground a direct data link to the drone (or manned plane) circling above. That would eliminate the multilayered, bureaucratic approach, in which information is often passed through IM windows and static-ridden radio connections. That same lone “Joint Terminal Attack Controller,” or JTAC, might be low-profile enough to slip into a situation like Libya without causing too much of an international ruckus.

The program to make this all happen is called Persistent Close Air Support, or PCAS. And the goal is to give that controller the ability to “request and control near-instantaneous airborne fire support.”

Darpa and the Air Force Research Lab recently handed out big contracts to the usual suspects — [Northrop Grumman](#) and [Raytheon](#) — for the next phase of the PCAS project.

But the military also gave a [million bucks to the relatively tiny Vuzix Corp.](#) of Rochester, New York. Which is a little odd, at first blush, because Vuzix is an [eyewear company](#), specializing in augmented reality specs.

DARPA's Hologram Goggles Will Unleash Drone Hell



But a little augmented reality may be just what a JTAC needs, in order to call in those airstrikes on his own. Rather than staring down at a bunch of maps and computer screens — and calling up intelligence analysts at headquarters for more info — it'd be better (and faster, and less prone to error) if he could get all of that data right on his augmented reality goggles. Oh, and if there was an integrated head-tracker, so the attached computer could basically see what the JTAC sees.

“It is all about speeding up the CAS [close air support] mission and eliminating friendly fire issues that can occur if the user on the ground may not have the whole picture of what is around them,” Vuzix executive Stephen Glaser tells Danger Room.

“The head tracker knows where the user is looking, so the information the user is seeing changes as he moves or turns his head. Theoretically you could look up in the sky and a little green triangle would appear telling you, you have an F-16 30 miles out at 21,000 feet. It could also tell you what type of ordnance the plane was carrying, so

DARPA's Hologram Goggles Will Unleash Drone Hell

you could make a quick decision if that plane would be appropriate for the mission.”

Some of this can be done today with pilots’ heads-up displays. But those require so much power and light, a JTAC would need to lug around an extra 8 pounds of batteries to make it work. (And it still wouldn’t work in direct sunlight.) That’s where the holograms come in.

Vuzix’s setup uses a more-or-less traditional microdisplay, then mates that up to a flat piece of glass called an [optical waveguide](#). The light from the display travels down the glass and bounces around inside the glass parallel flats. Those beams are directed to holographic film, which bounces the image to the eye.

If the plan works, the system will be tiny — just 3 mm thick. And when the display is off, it’ll be totally see-through. Glaser notes: “This will ultimately allow us to design the display right into a pair of sunglasses, so no one will know you are even wearing a display.” Which could make the goggles good for civilians, as well as troops ordering in a robotic, lethal hail.

Could 4G Wireless Plans Interfere with GPS?

Could 4G Wireless Plans Interfere With GPS?

By [John Reed](#) Friday, April 8th, 2011 11:54 am

A senior Air Force space official recently warned of the potential threat of 4G wireless service interfering with Global Positioning System transmissions.

One broadband company in particular, [LightSquared](#), has received temporary permission to build 40,000 ground-based transmitters “with exponentially more power, ones that transmit significantly closer to GPS receivers as compared to our transmitters that are 22,000 miles away in space,” said Lt. Gen. Michael Basla, the vice chief of Air Force Space Command during a cyberwarfare conference in Maryland. “So now we have a physics problem and a huge spectrum concern with potential GPS interference.”

This has the potential to disrupt not only GPS-based navigation but also the world’s satellite based timing signals on which “our networks, banking systems and power grids rely,” said Basla.

4G wireless is meant to provide IP-based broadband web service to the world’s mobile device users; this includes everything from laptops and tablets to smartphones, and yeah, it’s an understatement to say that this market is going to be huge.

The government is apparently looking into the issue to determine if the company can deploy this service without interfering with GPS signals, according to the three-star. “Believe me, I hope that is the case for both economic and operational reasons,” added Basla.

Meanwhile, the ageing GPS constellation itself is doing quite well due to the fact that it has recently been expanded to 24 satellites and is starting to be upgraded with the new Block IIF satellites.

“The GPS constellation is a model on the incremental capability for our space domain, we have replacements in the pipeline,” said Basla. “Our GPS constellation continues to exceed the requirements that our nation has placed on us.”

IBM's Watson Goes to College

IBM's Watson Goes to College

IBM takes its Watson supercomputer to college to play the "Jeopardy!" quiz game against students from Carnegie Mellon University and the University of Pittsburgh.

IBM is hosting a Watson symposium with [Carnegie Mellon University](#) and the [University of Pittsburgh](#), bringing together a group of academic minds to share ideas about the possibilities of Watson [technology](#) in the areas of medicine, law, business, computer science, engineering and more.

In addition, teams of students from CMU and the University of Pittsburgh will put their skills to the test in a demonstration of IBM Watson's question-and-answer capabilities. This is the first time students will have the chance to face Watson's powerful analytical capabilities in a practice round exhibition game of "Jeopardy!".

IBM chose to host the first Watson university symposium in Pittsburgh because of Carnegie Mellon's key contributions to the development of Watson—led by Eric Nyberg, professor, Language Technologies Institute, CMU School of Computer Science—and the university's role as a leading center for computer science research and education. In addition, the University of Pittsburgh has a long partnership with IBM in research projects such as [cloud computing](#), carbon nanotubes and smarter health care research around pandemic disease outbreaks and tissue regeneration.

By bringing this technology to the university community, IBM aims to inspire the next generation of innovators and entrepreneurs to think about how technologies such as Watson can benefit society, the company said. The event will also discuss the skills students need to drive future innovation.

"This is the first time we're bringing together Watson, IBM scientists, faculty and students to prepare for the next evolution in [computing](#)," said Bernie Meyerson, vice president of innovation and university programs for IBM, in a statement. "Watson will transform how technology is applied to assist doctors, business people and more. Our hope is that seeing Watson first-hand will spark innovation from the leaders of tomorrow so that together we can continue to build a smarter planet."

"Machines that think have been Carnegie Mellon's stock in trade since the first artificial intelligence program was invented here more than 50 years ago," said Jared L. Cohon, president of Carnegie Mellon University, in a

IBM's Watson Not as Smart as You Think

IBM's Watson not as smart as you think

But increasing compute power will mean 'smart' products for everyone, MIT prof says
Lucas Mearian

April 12, 2011 ([Computerworld](#))

CAMBRIDGE, MASS. -- As smart as IBM's Watson supercomputer may have seemed [while defeating two former Jeopardy champions](#), it wouldn't be able to hold a conversation with or speak intelligently to the attendees at its own conference, according to artificial intelligence (A.I.) experts who spoke at MIT Monday.

"Although Watson is a tremendous engineering achievement, there are some things it can't do," said Patrick Henry Winston, a professor and former director of the Massachusetts Institute of Technology's (MIT) Artificial Intelligence Laboratory. "For example, if there was a conference about Watson, Watson couldn't attend. It would have nothing to say about itself. It can't participate in discussions about how it works."

Winston was among dozens of researchers who spoke at MIT's [Computation and the Transformation of Practically Everything symposium](#), which is part of the school's 150-year anniversary celebration this year. The symposium continues today.

Winston pointed out that after computer scientists, such as James Slagle, began producing A.I. programs in the early 1960s, the scientific community and the public believed computers would have general intelligence within a few years. That didn't happen.

"Apparently what we forgot or overlooked is the idea that it's much harder to produce programs that have common sense than it is to produce programs that behave at expert levels in very narrow technical domains," he said.

[IBM's Watson computer](#) can answer questions posed in natural language in near real time. Unlike mainframe-style supercomputers of the past, Watson is made up of 90 IBM Power 750 Express servers powered by eight-core processors -- four in each machine, for a total of 32 processors per machine. The servers are virtualized using a Kernel-

IBM's Watson Not as Smart as You Think

based Virtual Machine (KVM) implementation, creating a server cluster with a total processing capacity of 80 teraflops. A teraflop is one trillion operations per second.

However, what Watson lacks is the [ability to connect life experiences to form cohesive thoughts](#), which is what gives humans their cognitive ability, Winston explained.

Ed Lazowska, who holds the Bill & Melinda Gates Chair in Computer Science & Engineering at the University of Washington, also took a shot at Watson.

Lazowska noted that after Watson's initial victory in February on *Jeopardy*, the machine was then handily defeated soon thereafter by Rep. Rush Holt, (D-N.J.), during a technology demonstration on Capital Hill. Holt, a nuclear physicist and five-time "Jeopardy" winner, beat the computer with a score of \$8,600 to \$6,200.

"It shows we need more physicists in Congress. Rush is the only one," Lazowska quipped.

While Watson may not be able to have an intelligent conversation, its appearance on "Jeopardy" heralded a sea change in A.I. brought about by multicore processors, clustered computing and sophisticated computer management software.

The computational power that got man to the moon in the late 1960s is now "embodied in [Furby](#)". "Admittedly, not the best use of that computational power," Lazowska said.

Ten years ago, one IT administrator was needed to manage 250 servers. Today, that person can manage thousands of servers. For example, Microsoft's Azure cloud computing platform requires only 12 support people for 35,000 servers divided between two continents, Lazowska said.

The exponential power behind computing has allowed the Internet to have a dramatic impact on our lives, more so than anything else in the past 40 years, he said. Over the next several years, consumers will see that power used to create smart homes, smart healthcare, smart robots and smart cars capable of reactive decision making, Lazowska said.

For example, today we're already seeing cars that can parallel park themselves and even navigate [rural](#) or [urban traffic](#) without a human driver.

IBM's Watson Not as Smart as You Think

The key to future computer development is "system building," where instead of technologists developing technology within their fields of expertise, they work in teams that include a variety of disciplines.

"When speech recognition and vision people get together, they're able to build system that provides dramatically greater capabilities than they could do on their own," he said.

Anant Agarwal, a professor in the MIT Electrical Engineering and Computer Sciences Department, said computers need to be more like humans if they're going to be able to take advantage of engineering advances.

Agarwal said his department's vision is to build a processor with hundreds or even thousands of cores, something that could be a reality in as little as four years.

One major obstacle to building multi-thousand-core processors is controlling heat generation from the circuitry. One way to control heat generation is to keep the cores as close to the DRAM memory as possible, thereby shortening the circuitry and reducing the time for heat to build. Another way is to balance application performance with hardware capability.

"We need to rethink compilers, operating systems, architectures, how we program computers; The first thing you want to do is to have applications be able to communicate their goals to the operating system," Agarwal said. "What we need is self-aware computation."

That would be like having an application "tell" an operating system what it needs in terms of processing power, and then having the OS balance that need with the needs of other applications running at the same time.

Agarwal noted that a human heart can communicate exactly what the body needs at any given point in time function optimally.

"If you're a good runner, your body temperature actually goes down the longer you run," he said. "If you're a computer, the longer you run the higher the temperature goes. So the question is, why can't computers become more like humans?"

IBM's Watson Not as Smart as You Think

Lucas Mearian covers storage, disaster recovery and business continuity, financial services infrastructure and health care IT for Computerworld.

IBM Shows Smallest, Fastest Graphene Processor

IBM shows smallest, fastest graphene processor

Agam Shah

April 7, 2011 ([IDG News Service](#))

IBM on Thursday demonstrated its fastest graphene transistor, which can execute 155 billion cycles per second, which is about 50% faster than previous experimental transistors shown by the company's researchers.

The transistor has a cut-off frequency of 155GHz, making it faster and more capable than the [100GHz graphene transistor shown by IBM in February last year](#), said Yu-Ming Lin, an [IBM](#) researcher.

The research also shows that high-performance, graphene-based transistors can be produced at low cost using standard semiconductor manufacturing processes, Lin said. That could pave the way for commercial production of graphene chips, though Lin could not say when manufacturing of such chips would begin.

Commercialized graphene transistors will provide a performance boost in applications related to wireless communications, networking, radar and imaging, said Phaedon Avouris, an IBM fellow. Graphene is a single-atom-thick layer of carbon atoms structured in a hexagonal honeycomb form.

The transistor was developed as part of research IBM is conducting for the U.S. Department of Defense's DARPA (Defense Advanced Research Projects Agency) program to develop high-performance RF (radio frequency) transistors. Avouris said the military has considerable interest in graphene transistors.

The flow of electrons is faster on graphene transistors than conventional transistors, which enables faster data transfers between chips, Lin said. That makes it promising technology for applications such as networking that require communications at fast speeds and high frequencies.

Graphene transistors may be able compute faster than conventional transistors, but

IBM Shows Smallest, Fastest Graphene Processor

are not ideal for PCs yet, Lin said. Because of the lack of energy gap in natural graphene, graphene transistors do not possess the on-off ratio required for digital switching operations, which makes conventional processors better at processing discrete digital signals.

By contrast, the continuous energy flow makes graphene better at processing analog signals, Lin said. Graphene's high electron speed allows for faster processing of applications in analog electronics where such a high on-off ratio is not needed.

The graphene transistor benefited from the use of a new and improved substrate IBM called "diamond-like carbon." The graphene transistor exhibited excellent temperature stability from room temperature down to minus 268 degrees Celsius, which the company called "helium temperature."

"The performance of these graphene devices exhibited excellent temperature stability ... a behavior that largely benefited from the use of a novel substrate of diamond-like carbon," IBM said.

The graphene transistor is also IBM's smallest transistor to date, researchers said. The gate length of the radio-frequency graphene transistor was scaled down from 550 nanometers to 40 nanometers, compared to [the gate length of 240 nanometers for the graphene transistor shown last year](#), which used a silicon carbide substrate.

But more importantly, the performance was achieved using manufacturing technologies compatible with those used in silicon device fabrication, Lin said. That brings the commercial production of graphene chips one step closer to reality, Lin said.

The possibilities of graphene have proved attractive to scientists. Andre Geim and Konstantin Novoselov of the University of Manchester in the U.K. were awarded the 2010 Nobel Prize in Physics for their groundbreaking research in graphene. The scientists isolated graphene in 2004, which laid the groundwork for further research.

Graphene holds great potential for semiconductors, but the industry is still trying to understand its benefits, said Jim McGregor, chief technology strategist at In-Stat.

IBM Shows Smallest, Fastest Graphene Processor

Graphene cannot yet operate as a digital transistor replacement in conventional silicon chips. However, it could be beneficial as a complementary technology in other carbon-based devices for tasks like signal processing.

"Like any new materials technology, it takes billions of investment dollars to make it a viable alternative to existing technology. Then again, it may eventually be a necessity if the current materials technology hits another physics brick wall," McGregor said.

Graphene has to fit into the three primary pillars of semiconductor manufacturing, which are materials, transistor design and lithography, McGregor said.

"If graphene can be supported through existing and future lithography processes and transistor designs, then it could be a viable materials technology, but only if those two conditions are satisfied," McGregor said.

US Navy's Laser Test Could Put Heat on Pirates

US Navy's Laser Test Could Put Heat On Pirates

(ASSOCIATED PRESS 13 APR 11) ... Jason Straziuso

NAIROBI, Kenya – A ship-based laser tested by the Navy's research arm could put the heat on Somali pirates.

The Navy for the first time last week successfully tested a solid-state high-energy laser from a ship. The beam, which was aimed at a boat moving through turbulent Pacific Ocean waters, set the target's engine on fire.

The Office of Naval Research says the laser traveled over "miles, not yards." For now, the test is a proof of concept, and it's not yet known when it might be deployed as a weapon.

The baseball-sized laser beam, though, could be used to stop small crafts from approaching naval ships. It could also target pirates.

"You can use the laser to ward off an attack, or you can dial it down to a non-lethal level where it basically becomes a very bright light so they know they are being targeted," Michael Deitchman, the director of air warfare and weapons at the Office of Naval Research, said Wednesday.

Deitchman said the laser provides two benefits not seen in other military weapons. The laser is precise, unlike bullets that can ricochet and hit unintended targets, and the laser's strength can be dialed down from a lethal level to a nuisance level.

Graeme Gibbon-Brooks, the head of Dryad Maritime Intelligence, said the test was "remarkable" for how the Navy was able to concentrate the beam over such a long distance at sea, and given how the boat was being tossed about in rough water.

"Hats off to the U.S. Navy because that is very, very impressive," he said. "It was pitching and rolling and yet they got this very fine beam to focus on one part of an engine casing. That they managed to keep the energy in one place is remarkable."

Somali pirates attacks have become increasingly violent in recent months. Pirate assaults typically involve multiple skiffs zooming in on a target. The pirates often carry and fire AK-47 assault rifles and rocket-propelled grenades at targets.

Some cargo ships now carry private security guards to defend against pirates. They also can use such defensive measures as water cannons and sound blasters. But those measures may not be enough to overcome an armed attack.

Gibbon-Brooks said the new laser "absolutely" could be deployed against pirates, but says a sniper rifle could work just as well. He suspects the Navy has bigger hopes for its sea-based laser. The Navy released a video of the test on YouTube. It's been viewed more than 600,000 times.

"It's a very, very interesting moment for naval warfare in that we have a whole new genre of weapons," he said.

"It's certainly a remarkable step forward. The ability to apply more power in a burst or the ability to manipulate that power is really where I see this going," he said. "I think if you watch the video and think that's what they intend to do to Somali pirates in a year, you don't understand what's being set out in front of them. It could be used in any type of naval warfare."

US Navy's Laser Test Could Put Heat on Pirates

The laser test was carried out by the Navy and Northrop Grumman as part of a \$98 million contract.

The Office of Naval Research's big project is a megawatt-level electron laser that could be used to defend Naval ships against supersonic and ballistic missiles, said Deitchman. The recent laser test helps the Navy move in that direction.

"It demonstrated once and for all that we could get material damage effects with a laser at sea, and it really gives us confidence to proceed on with directed energy systems," Deitchman said.

Airborne Radar Will Map the Ground in 3D

Airborne radar will map the ground in 3D

08 April 2011 by [David Hambling](#)

A SOFTWARE upgrade to existing radar systems will allow aircraft to map landscapes and buildings in 3D, and make it easier to spot part-hidden objects on the ground.

The software augments synthetic aperture radar (SAR), a technique that has been around since the 1950s. Airborne SAR works by sending radar signals towards each spot on the ground from several different points along a plane's flight path. Signals bouncing back from a particular object on the ground are combined to create a 2D image as if it had been taken from a single viewpoint - and in more detail than would be possible from a single source.

In the new approach, being developed in a project called Exploitation of Geometric Diversity, the aircraft flies in a curved or circular path rather than a straight line. This provides a series of images of the same object on the ground from a number of slightly different viewpoints, providing detailed depth information about the object. Software then produces a 3D image from the returning signals.

This is similar to the way stereoscopic photography and 3D movies use two images of the same thing taken at different angles to give the appearance of depth. Each pass only provides a small amount of data, but this can be built up over multiple passes.

Details of the project appear in US air force contracts awarded to two US companies under the Small Business Innovation Research programme.

"If enough fly-bys are collected, with lots of arcs, full tomographic imaging can be carried out, akin to medical imaging," says Keith Morrison, who

Airborne Radar Will Map the Ground in 3D

investigates radar techniques at Cranfield University in the UK. "You can create an image slice-by-slice in height, and run it as a movie just like a medical image through a brain scan."

This could be used, for example, to locate a crashed aircraft hidden beneath a forest canopy. Some 2D radar systems are able to penetrate foliage, but they often produce a noisy image with a lot of "clutter", as signals from the trees and objects on the ground are combined in a single image. The new 3D radar's software could "strip off" the forest canopy, to get a much clearer image of any object on the ground.

3D radar could also be used to map the insides of buildings - so long as the building does not have a metal roof that would reflect the radar signal - or measure the thickness of ice sheets or oil slicks.

The curved flight path also greatly improves the chances of picking up "glints" - strong radar reflections from certain angles that may reveal the location of objects that would otherwise be invisible. Initially, the 3D radar will be carried on Predator drones. Trials are expected to be completed by 2013.

To convert conventional SAR radar reflections into a single image, Predators already carry signal-processing hardware with computing power equivalent to about 100 PCs. The new approach will require even more powerful signal processing to return a usable 3D image in a reasonable time.

Batteries That Recharge in Seconds

Batteries that Recharge in Seconds

A new process could let your laptop and cell phone recharge a hundred times faster than they do now.

By Katherine Bourzac

A new way of making battery electrodes based on nanostructured metal foams has been used to make a lithium-ion battery that can be 90 percent charged in two minutes. If the method can be commercialized, it could lead to laptops that charge in a few minutes or cell phones that charge in 30 seconds.

The methods used to make the ultrafast-charging electrodes are compatible with a range of battery chemistries; the researchers have also used them to make nickel-metal-hydride batteries, the kind commonly used in hybrid and electric vehicles.

How fast a battery can charge up and then release that power is primarily limited by the movement of electrons and ions into and out of the cathode, the electrode that is negative during recharging. Researchers have been trying to use nanostructured materials to improve the process, but there's usually a trade-off between total energy storage capacity (which determines how long a battery can run before needing a recharge) and charge rates. "People solved half the problem," says **Paul Braun**, professor of materials science and engineering at the University of Illinois at Urbana-Champaign.

Braun's group has made highly porous metal foams coated with a large amount of active battery materials. The metal provides high electrical conductivity, and even though it's porous, the structure holds enough active material to store a sufficient amount of energy. The pores allow for ions to move about unimpeded.

The first step in making the cathodes is to create a slurry of polymer spheres on the surface of a conductive substrate. Because of their shape and surface charge, the spheres self-assemble into a regular pattern. The Illinois researchers then use a common technique called electroplating to fill the space between the spheres with nickel. Next, they dissolve the polymer spheres, and most of the metal, to leave a nickel sponge that's about 90 percent open space. Finally, they grow the active material on top of the sponge.

"It's some distance to a product, but we have pretty good lab demos" with nickel-metal-

Batteries That Recharge in Seconds

hydride and lithium-ion batteries, says Braun. The Illinois group has made lithium-ion batteries that charge almost entirely in about two minutes. The method should be applicable to the cell sizes needed for laptops and electric cars, though the researchers have not made them yet.

"The performance they got is unprecedented," says Andreas Stein, a professor of chemistry at the University of Minnesota. Stein pioneered the polymer-particle templating method that Braun's group used. Braun's work is described in the journal *Nature Nanotechnology*.

Jeff Dahn, professor of physics at Dalhousie University, is skeptical that these electrodes will ever end up in products. "When you look at the flow chart for making this structure, it's pretty complicated, and that is going to be expensive," he says.

Braun acknowledges: "There are lots of people coming up with elegant [electrode] structures, but manufacturing them is tricky." He says, however, that his fabrication process combines existing methods that are currently widely used to make other products, if not to make batteries, and that it shouldn't be too difficult to adapt them. The process would add extra steps to making a battery, but these steps aren't particularly expensive or complex, Braun says.

Braun's group will next test the electrode structure with a wider range of battery chemistries and work on improving batteries' other half, the anode—a trickier project.