Cyber Bytes - 24 JUN 11

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

Links of interest:


Cloud Computing

Improving the Security of Cloud Computing
-<http://www.technologyreview.com/business/37683/?ref=rss>

Want a Military iCloud? Then Reduce Bandwidth Drain

Cyber Security

Hackers and Clouds: How Secure Is the Web? [audio]

Is it time RSA to Open Up About SecurID Hack?
-<http://www.computerworld.com/s/article/9217551/Is_it_time_for_RSA_to_open_up_about_SecurID_hack?
source=rss_latest_content&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+computerworld%2Fnews%2Ffeed+%28Latest+from+Computerworld%29>

Navy Begins Routine Cyber Security Inspections [audio]

Who's Behind the Hacks?
Prepare for the 'Advanced Persistent Threat'
<http://www.technologyreview.com/business/37767/?ref=rss>

For Recent Cyber Attacks, Motivations Vary [audio]

Pentagon's Advanced Research Arm Tackles Cyberspace
<http://www.reuters.com/article/2011/06/16/us-usa-cybersecurity-attacks-idUSTRE75F5RY20110616>

Hackers Declare War on Government Agencies

Kindergarten-Level Computer Security
<http://www.technologyreview.com/business/37838/?ref=rss>

Inside the Anonymous Army of 'Hacktivist' Attackers
<http://online.wsj.com/article/SB10001424052702304887904576399871831156018.html?mod=WSJ_Tech_LEADTop>

LulzSec? Anonymous? Know Your Hackers
<http://www.pcmag.com/article2/0,2817,2387396,00.asp>

No Easy Answers to Password Problems
<http://www.technologyreview.com/business/37837/>

Password Cracking, Mining, and GPUs

Botclouds: A Cyber Attacker's Dream
<http://www.newscientist.com/article/mg21028175.500-botclouds-a-cyberattackers-dream.html>

NSA Allies With Internet Carriers to Thwart Cyber Attacks Against Defense Firms

Is Cyber Crisis the New 'Normal'?
Old Worm Won't Die After 2008 Attack on Military
<http://www.reuters.com/article/2011/06/17/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617>

Cyber War

US, China Need Cyber Detente
<http://www.reuters.com/article/2011/06/14/us-china-kissinger-cyber-idUSTRE75D62Q20110614>

China's Cyberassault on America
<http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html>

Chinese Military Warns of US Cyberwar Threat

New Leader for Navy's Cyber Forces as Pentagon Gets Cyberwar Guidelines

China Says No Cyber Warfare with US
<http://news.yahoo.com/s/nm/20110622/tc_nm/us_china_usa_cyberwar;_ylt=Agkewf5I72VUVP_DjCuSNNVT.3QA;_ylu=X3oDMTJzMW9kZG8yBGFzc2V0A25tLzlwMTEwNjlyL3VzX2NoaW5hX5hX3VzYV9jeWJlcnndcgcRwb3MDMTAEc2VjA3luX3BhZ2luYXRlX3N1bW1hc3JfGlzdAARzbGsdY2hpbmFzYXJlbm9j>

US Building Virtual Internet As Cyberattack Testbed

Is This the Start of Cyber Warfare?

DoD

Navy Must Cut IT Business Systems Spending by 25%
<http://www.federalnewsradio.com/?nid=35&sid=2417374>
Navy Goes Full Speed Ahead With Next-Gen IT Projects

Navy Faces Headwinds in Critical IT Plans

HP Orders Worth $1 Billion At Risk As Navy Takes Over Intranet
-<http://www.bgov.com/news_item/aQLg8mm1s0qCB0Qg4gha_g>

The Army's Big Network Experiment

Navy: Actually, Most Military Intel Systems Suck

DISA Eyes Central Management of 1 Million Cell Phones and Other Wireless Devices

DISA Promotes Remote Access for DoD Computers

CYBERCOM, Geographic Combatant Command Roles Unclear, Finds GAO

Navy To Make Downselect Decision For CANES Prime Contractor By December
-<www.defensedaily.com/publications/dd/14326.html>

DoD Must Unify Maritime Domain Awareness Efforts, Says GAO

Power Down: Senate Zaps Navy's Superlaser, Rail Gun

Info Dominance Vital to the 'Kill Chain," Navy Intell Czar Says
Information & Society

ONR Announces Multimillion-Dollar 'STEM Grand Challenge'

Obama: 'We Don't Have Enough Engineers'
-<http://www.computerworld.com/s/article/9217624/Obama_We_don_t_have_enough_engineers_>

Navy Officers Fall Prey to the Thin Digital Line Between Personal & Professional Lives

Somali Pirates Go High Tech

Information Technology

IPv4 to IPv6 Switch: When Protocols Collide

Welcome to a Faster Web
-<http://www.technologyreview.com/web/37772/?ref=rss&a=f>

IPv6: Come On In, The Water's Fine

Cyber Wargamers Set Sail Against Pirates

RIM PlayBook Holds Security Edge Evan As iPad Wows US Troops

The Web Is Shrinking. Now What?
-<http://allthingsd.com/20110623/the-web-is-shrinking-now-what/>
Web Addresses Enter New Era
<http://online.wsj.com/article/SB10001424052702303936704576396963900727284.html>

Loosen the Cap on Employees' In-Boxes
<http://www.technologyreview.com/business/37886/?ref=rss>

Robotics

Fire Scout Proves Worth

Remotely Piloted Aircraft Fuel Demand for Satellite Bandwidth

U.S. Navy Eyes Submarine-UUV Mix

War Evolves With Drones, Some Tiny as Bugs

Space

Russia May Target US Sats With Laser Jet
<http://www.wired.com/dangerroom/2011/06/is-a-russian-laser-aiming-for-u-s-satellites/>

After Delay, Iranians Launch a Satellite
<http://www.nytimes.com/2011/06/16/world/middleeast/16iran.html?_r=2>

Astrobotic, CMU Build Lunar Lander in X Prize Bid [video]

Seven Questions for Iridium...
<http://allthingsd.com/20110621/seven-questions-for-iridium-ceo-matthew-desch-yes-
New LightSquared Plan to Reduce GPS Interference Greeted With Skepticism at House Hearing

Technology Advances

A Preview of Future Disk Drives
-<http://www.technologyreview.com/computing/37771/?ref=rss>

The 10 Strangest Facts About Graphene

Japanese 'K' Computer Is Ranked Most Powerful
-<http://www.nytimes.com/2011/06/20/technology/20computer.html?_r=1>

Genius Computer Stops Rockets 'Right' Before Impact [video] [Iron Curtain Active Protection System]

When the Problem Is the Problem [Recalling lessons from Manhattan Project's, Bell Labs', and NPS' Richard Hamming]

Accelerating Cutting Edge Technology Manufacturing [New White House Initiative]
-<http://www.post-gazette.com/pg/11175/1155959-100.stm>
Improving the Security of Cloud Computing

Wednesday, June 15, 2011

Improving the Security of Cloud Computing
Solutions emerge to guard against attacks and data loss in the cloud.
By David Talbot

On-demand cloud computing and data storage can save companies money, but many businesses—particularly in finance and health care—are wary of handing data to third parties, fearing hacking, accidental data loss, or theft by rogue employees of cloud providers.

New security solutions are appearing: One verifies cloud providers' claims that your data is safely lodged on its own server. Another protects your cloud-based data by using a math function to divide it into 16 segments, any 10 of which can be used to re-create the entire original set.

The first of these solutions responds to recent demonstrations that hacking within clouds—using one set of rented computers or "virtual machines" to attack another—is theoretically possible. In 2009, computer scientists at the University of California, San Diego and MIT showed how an attacker using Amazon's Elastic Compute Cloud could land on the same physical server as his intended victim. (In one method, they forced a hypothetical victim to hire more virtual machines by bombarding his website with traffic and then created attacking virtual machines at the same time. This put the two sets of machines on the same cloud server 40 percent of the time.)

The researchers also pointed out that attackers who sat on the same servers as victims could do things like monitor usage of shared physical resources, such as the server's central processing unit (CPU), to infer information such as what kinds of programs the victim was running and how much Web traffic the victim was handling. These actions are known as "side-channel" attacks.

Amazon, in a move similar to ones made by other cloud providers, now offers a virtual private cloud service in which a customer is promised his own isolated server. Because customers are likely to want to confirm that they're getting what they paid for, a group of researchers at RSA Laboratories, in Cambridge, Massachusetts, and the University of North Carolina at Chapel Hill has developed a verification method that involves monitoring a piece of shared server hardware called the CPU cache, which allows quick access to frequently tapped memory resources. The prototype technology lets a client monitor whether the CPU cache on its cloud server is doing anything beyond what would be expected by the client's own computation. Such a discovery
would suggest that someone else is sharing the server. "This allows you to check on your situation in the cloud," says Thomas Ristenpart, a computer scientist at the University of Wisconsin, Madison, and a coauthor of the paper that described the Amazon weakness. "It's a way of doing detection on when you actually have a physical server to yourself."

The tool worked 85 percent of the time in tests and is being refined before commercialization or licensing, says Alina Oprea, a research scientist at RSA Labs, who cowrote the software. "The tenant can run this protocol without the help of the cloud provider. This would give them stronger guarantees," she says. Similar approaches under development could monitor other shared hardware elements, such as hard drives, she adds.

Companies also want to ensure that their remotely stored information won't be corrupted, lost, or stolen. Encrypting data before storing it can help, but this requires keeping track of encryption keys and monitoring new technologies for their potential to break the encryption. (On the plus side, a future system might allow you to actually compute with encrypted data, infeasible with current technology.)

These downsides of encryption can be avoided with a newly commercialized technology that provides a mathematical way of slicing your data into 16 parts before storing it. It employs a fancier version of algebraic equations (in which knowing two parts of an equation lets you solve for the third) to let you reconstitute your full data set from any 10 of those 16 slices.

This process does increase the amount of data you need to store by between 30 percent and 60 percent, but that's more efficient than some encryption methods. And if you distribute your 16 slices among different storage providers, "you can build systems where you don't have to trust the service providers," says Chris Gladwin, CEO of Cleversafe, the Chicago company that launched the software late last year. "They can tamper, lose, or steal it and it doesn't matter if they steal below a threshold."

Other technologies are in the works to make cloud computing more secure, because no one doubts that as data moves to clouds, so will hackers and criminals. "Anyone can use Amazon," Ristenpart says, "so criminals have access to it as well."
Want a Military iCloud? Then Reduce Bandwidth Drain

• By Spencer Ackerman June 15, 2011 | 2:55 pm | Categories: Info War @attackerman · 10.9K followers

It’s not just Steve Jobs who’s promoting storing your data in the cloud. The mad scientists at Darpa want a secure cloud for the military. Their counterparts at the Office of Naval Research are moving in the same direction.

Just one problem. Unlike Apple, the military’s networks are going to have to work in low-bandwidth environments, like the Afghan mountains, under the oceans or even Antarctica. There’s more data to share than there is bandwidth to carry it all. That’s where a European company called Infonic comes in.

Infonics created a software solution called Geo-Replicator that allows users of military networks to share data while cutting down on bandwidth-draining redundancies. The idea is that low connectivity environments don’t have to be isolated nodes in the military net. That way, “the network doesn’t become the barrier to sharing information,” says Lawrence Poynter, Infonics’ chief technology officer.

Poynter spoke from the Naval Space and Naval Warfare Systems Command’s San Diego laboratory, where he’s showing a test of the software that purports to get data around networks running as slow as 2 kilobytes per second. The Navy’s been a customer of Infonic’s products for the last eight years. Its software helps the Navy’s “Distance Support” network keep technicians out at sea connected to maintenance manuals for complex naval systems. Same thing with the Marine Corps.

An anecdote Poynter shares explains the gist behind Geo-Replicator. Not long ago, a NATO commander in Germany wanted to send his subordinates daily updates to “a beast” of a PowerPoint presentation sized at 50 megabytes. “It froze the network.
Want a Military iCloud? Then Reduce Bandwidth Drain

Everyone was trying to download 50 megabytes of content," he recalls. He ran the same file out through Geo-Replicator, and the software searched for redundant data between the last version of the PowerPoint and the new update, sending out only the new stuff.

All that transmitted was in the low tens of kilobytes. But “once you transmitted the update file, you then regenerated a 50 megabyte PowerPoint file, and everyone could read that local file. All that bandwidth traffic zapped out,” Poynter says.

And that’s in highly-connected Germany. Ultimately, NATO’s Document Handling System will use Geo-Replicator to push information out to Gen. David Petraeus’ headquarters in Kabul and then “down to the FOBs,” the bases in remote areas of Afghanistan, Poynter says.

Not that troops necessarily need more access to PowerPoint presentations. But if the military’s increasingly looking to the cloud to store its data, and push it out to mobile devices like smartphones, Infonic’s method of trimming out the fat clogging the bandwidth arteries might be worth studying.
Two new victims took a hit in the Wild West world of computer hacking this week: Citibank, where 200,000 credit card holders were victimized, and the International Monetary Fund, which reportedly also endured a cyberattack.

The FBI is on the case — so much so that 1 in 4 hackers may now be an informant, according to some experts.

Ed Pilkington, who covers hacking for the Guardian, tells Weekend All Things Considered guest host Rachel Martin that the overriding atmosphere in the hacker community is one of paranoia and fear as more and more of them join the other side to get out of trouble.

"They don't really who know who's doing what," he says. "It seems such an extraordinary contradiction. Here is this community which in popular vision is a community of anarchists, anti-establishment people, and yet here are so many of them actually acting as the eyes and ears, as virtual spies, on behalf of FBI and Secret Service."

There are those in the cyber-community who think even more than 1 in 4 hackers are in cahoots with the U.S. government these days. Former hacker and information security consultant Kevin Mitnick says that informants are essential to America's defenses.

"I don't know of any case that involves computer hacking where there were multiple defendants charged where there wasn't an informant on the case," he says.

Here is this community which in popular vision is a community of anarchists, anti-
establishment people, and yet here are so many of them acting as the eyes and hears on behalf of the Secret Service.

- Ed Pilkington, journalist

And Mitnick knows the community well. As a kid, he found he had a knack for what was then called "phone freaking" — essentially hacking phones before there were computers.

"When I got pretty adept with manipulating the phone company's systems, I was able to pull pranks," Mitnick says. "I was able to change a friend's home telephone's class of service to that of a payphone. So whenever he or his parents would pick up the phone to make a call, it would say, 'The call you have made requires a 25 cent deposit.'"

Years later, Mitnick went from hacking phones to breaking into phone companies' computer systems. Then in 1995, he was arrested on charges of computer fraud and served a five-year jail sentence. A fellow hacker testified against him in court in exchange for a lesser sentence.

"You definitely feel a great sense of betrayal," Mitnick says of the testimony. "If hackers, if anyone committing a criminal act, wants to reduce their risk, they obviously don't involve anybody else. The greater the circle of people that know what you're doing, the higher the risk."

Catching Small Fish

Today, the risk — and the stakes — have never been higher. As more and more personal and financial information has wound up on the Web, hackers have increasingly banded together to attack that information.

"The main group are the carders. They specialize in breaking into databases of credit cards, usually held by banks or credit card companies," Pilkington says. "They can do millions of dollars of damage in terms of stealing directly from bank accounts, or going
out with fraudulent credit cards that they create using this database of information."

They do this with very sophisticated attacks. But the FBI has managed to fight them, Pilkington says, using an old-fashioned trick.

"It's the trick they use against drug gangs, it's the trick they use against mobsters and the mafia: You catch a little guy doing a little thing," he says.

Pilkington gives the example of Albert Gonzales, who was caught fraudulently taking money out of an ATM, which "in the scheme of this stuff is pretty small beer." Authorities got him out of prison early and set him up in an FBI office. They paid him $75,000 a year to set up networks to meet other hackers.

"He then became essentially a honey trap for big carders and identity thieves in the hacking community," Pilkington says.

But last year Gonzales got a 20-year sentence for hacking: While he was working as an informant for the FBI, he was secretly hacking government agencies and bank accounts.

Fifteen years ago, Mitnick says, things were not this complicated.

"When I was a hacker it was all about pursuit of knowledge, getting a bite of the forbidden apple, so to speak. Then of course the challenge and the seduction of adventure," he says. "Today it's all changed. I mean, the trend of hacking today is all profit — credit card numbers, bank account numbers. For example, Sony recently has suffered over 17 attacks."

**Protecting The Cloud**

Another tech company hackers were watching closely this week was Apple. CEO Steve Jobs announced the iCloud, a new service that will allow Apple users to store all
their email, photos, music and documents on an array of servers.

"By centralizing their data, they've really painted a target on their back," says David Brumley, a computer scientist at Carnegie Mellon University in Pittsburgh. He says Apple's iCloud is a bank of servers in a building the size of two football fields in North Carolina.

"From the reports, they have barbed wire around the building, they have guards and you're going to need an ID to get into those buildings," he says. "So the physical security is actually pretty good. It would be a lot like getting onto a military installation to actually get into Apple's iCloud data center."

Though it may be tough to break into the server's headquarters, Mitnick says, breaking in online could be another story.

"I was hired to test this cloud infrastructure in South America. Literally in the 15 minutes that I was on the phone with the CEO of the company and one of the lead technical guys, I was able to get access that only system administrators should get access to," he says.

Mitnick says there are things everyday Internet users can do to protect their information, like using a VPN client or more secure browsers like Google Chrome, but he adds, "Anything out there is vulnerable to attack given enough time and resources
Is it time for RSA to open up about SecurID hack?

Robert McMillan

June 10, 2011  (IDG News Service)

For any company that makes its living selling security, it's a nightmare come true. This week, RSA Security admitted that hackers who broke into its network three months ago had stolen information about its SecurID tokens and then used that information to attack a customer, Lockheed Martin.

RSA seems to think the vast majority of its customers aren't directly threatened by the hacking incident, but the company's reputation has taken a hit. And users and pundits alike have blasted RSA for not being clear about exactly what was taken, and how it could affect them.

Calls for more disclosure about the March hacking incident only got louder this week, after Lockheed Martin confirmed that it was reissuing RSA tokens company-wide in response to the attack, and after RSA began offering to replace tokens for any customers who asked.

By not disclosing what happened, RSA is making it hard for customers to understand the risks they face and make informed decisions, said Thierry Zoller, practice lead for Verizon Business Luxembourg. "It's time for them to come clean," he said. "By not coming clean they are creating more fear, uncertainty and doubt than necessary."

RSA has said the hackers were sophisticated, but it has been vague about what exactly they managed to steal. The best the company could do this week was to confirm that "the attack resulted in certain information being extracted from RSA's systems that is related to RSA SecurID multi-factor authentication products."

Even without a clear answer from RSA, some security experts took the Lockheed Martin incident as proof that the hackers who broke into RSA's systems are now able to clone SecurID tokens and use them to break into networks.
Is it time RSA to Open Up About SecurID Hack?

If that were true, here's how an attack might work.

Attackers appear to have gained access to RSA's database of seed numbers, called "token records" in RSA parlance. These numbers are essentially the building blocks used to create the six-digit log-in numbers that RSA tokens generate every sixty seconds or so. The tokens are widely used by governments, contractors and banks to add a second layer of security alongside computer passwords.

With a seed number in hand, a technically savvy hacker could figure out what log-in number a SecurID token would generate at any given time. The trick, however, would be to figure out which particular token a victim was using. That's not obvious. RSA says it has shipped about 40 million tokens, so it would take some work to link a particular seed number to a particular user's SecurID token.

A criminal might be able to achieve this by posing as a network administrator and emailing a victim, telling them to visit a Web site and to log in with their password and SecurID login number. With just a couple of successive log-ins, hackers could figure out which of the millions of seed numbers was used to generate the log-in numbers. Or they could identify the seed numbers by asking victims to enter their tokens' serial numbers, say as part of a security audit, and then look that serial number up in their stolen database.

Whether all RSA customers need to worry about this type of attack is unclear. It may be that whoever hacked the company was only looking for seed numbers associated with a particular customer – Lockheed Martin, for example. It could also be the case that the hacker is about to publish all of the seed numbers on a public website, sending all SecurID customers scrambling for cover. It may be that RSA doesn't actually know how much data was taken.

The lack of a clear explanation has led to a lot of chatter among security experts.

"The RSA situation has been going on for a couple months now, with no shortage of rumors swirling about what was lost, and no real guidance from RSA on the risk to their customers (at least none outside of NDA)," wrote Dan Kaminsky, an independent security researcher, in a recent analysis.
The confusion has caused some perception problems for RSA about its products, said the chief security officer at one company who spoke on condition of anonymity because he didn't want to jeopardize his company's relationship with RSA's parent company, EMC. "As a buyer right now, their name is just something I'd stay away from," he said. "Do you want to tie your reputation to them and not know enough?"

RSA said it can't say any more about what was taken, or by whom, for "security reasons." People familiar with the situation said disclosing exactly what data was taken could potentially harm the reputation of some RSA customers, which is something RSA is taking pains to avoid.

Christopher Ipsen, chief information security officer for the State of Nevada, said his organization plans to take RSA up on its offer to reissue SecurID tokens. But he said he understands why RSA might be reluctant to release details of the attack. "You don't want to give too much information out about the exploit," he said. "But there is an appropriate time when full disclosure is imperative."

Three months after the RSA attack, how far away is that "appropriate time"?

"I think we're really close," Ipsen said.

Robert McMillan covers computer security and general technology breaking news for The IDG News Service. Follow Robert on Twitter at @bobmcmillan. Robert's e-mail address is robert_mcmillan@idg.com
Navy Begins Routine Cyber Security Inspections

Navy Begins Routine Cybersecurity Inspections
(FEDERAL NEWS RADIO 13 JUN 11) ... Jared Serbu

Naval personnel who have long been accustomed to the idea of being regularly examined on physical security, training, safety and a host of other issues will soon have to get used to "stem to stern" inspections in one more category: cybersecurity.

While the notion of defending data and the systems that contain it is not new in the military services, a regime of inspections focused specifically on IT security is, said Rear Admiral Ned Deets, commander of the Naval Network Warfare Command.

He said it's a program the Navy simply has not invested in until recently.

"We've never had an inspection force. We do now—nascent, but growing," he said. "We've built an inspection plan that will eventually inspect, on a three year cycle, 900 command units across the Navy. It looks a lot like a lot of the other inspection programs we have across the Navy, like INSURV and things of that nature."

Each year, Deets said, every one of the 900 commands should expect to be subjected to some sort of cybersecurity inspection.

"We'll do an administrative inspection to take a look at your program first," he said. "Second will be unit-level training and advice and assistance to ensure that you're ready to operate in your unit, and third will be a stem-to-stern inspection of everything associated with your networks and long-haul communications, physical security included. In the Navy, we expect what we inspect, and we have never inspected in this area before."

Deets, who spoke last week at AFCEA Northern Virginia's Naval IT day, said the inspections are one step the Navy is taking to try to get its personnel to think of the service's IT systems as warfighting tools, and to treat them accordingly.

Admiral Jonathan Greenert, the Navy's vice chief of naval operations, said that mindset is still not prevalent enough in the Navy. He said while the service has no shortage of good security hygiene procedures in its rulebooks, they're too often ignored.

"The network security posture is still not on a lot of commanders' daily reports, and it really needs to be," Greenert said. "The workforce awareness is pretty low on information assurance. We still need to go in and slap people's hands, because they want to plug things like thumb drive into our computers or they want to charge their iPads. We're not really complying yet with the existing security directives, and up to nine out of ten of the exploits that we've had have been known vulnerabilities. They could have been cut off."

But even if the vast majority of the IT security problems the Navy has identified are related to conduct and culture, those two factors alone don't account for all the service's weaknesses, according to Deets. He said the Navy lacks the ability to oversee and defend its networks to the degree it would like to, in part, because there are so many of them.

To deal with that, the Navy is in the process of weeding through older legacy networks, and either shutting them down or folding them into one of the Navy's three primary and more modern IT networks.
Navy Begins Routine Cyber Security Inspections

Deets says they began the project with about 1,000 networks, which they have reduced to 348. "That will go down further," he said. "This is one of those areas where we have to succeed. The fewer number of networks that we're attempting to manage and secure out there, the better. I don't want it down to a single network. That becomes way too easy to predict and attack. But I've got to get it down below 348. That's a hard number to manage."

Listen To Audio (RT: 4:57)
Who's Behind the Hacks?

JUNE 14, 2011 1:33 PM PDT
Who is behind the hacks? (FAQ)
by Elinor Mills

Every day there's another report of a computer hack. Yesterday it was a video game company and a U.S. Senate database. And today it could be the Federal Reserve. There's no doubt that there's a wave of attacks going on right now, against different targets and with seemingly different motives.

The questions on everyone's mind are who is behind these computer attacks and why are they doing it. This FAQ will help answer those questions in at least some of the cases.

**Who is Anonymous?**

Anonymous is the best known of the groups that are currently active and publicly taking credit for, even publicizing in advance, attacks on Web sites. It's a decentralized group that specializes in organizing distributed denial-of-service (DDoS) attacks designed to shut down sites, particularly in support of freedom of speech. Past targets have included the Church of Scientology, BMI, the governments of Egypt and Iran, and companies owned by conservative activist billionaires Charles and David Koch. They also conducted a massive compromise of the security firm HBGary Federal, which had reportedly been working with the FBI to identify the leaders of Anonymous.

They launched a series of effective DDoS attacks against PayPal, Visa, and MasterCard late last year after the companies stopped enabling WikiLeaks to receive contributions through those means. Sources told CNET that the group has undergone a loss of membership and radical shift in direction and organizational participation.
Who's Behind the Hacks?

since the arrest of a 16-year-old alleged member in the Netherlands late last year, the arrest of five people (ages 15-26) in the U.K. in January, and the issuing of more than 40 arrest warrants in the U.S. Member identities were reportedly leaked on the Internet as well. The group's strong anti-establishment and political messages have led some to call them hacktivists, which refers to activists who hack. It's unclear how many people participated in their campaigns, which they call "operations," because their system is designed to allow for confidential participation.

Who have they targeted recently and why?
Anonymous pretty much started the recent spate of hackings against Sony, hitting several Sony sites with a DDoS in early April in retaliation for Sony taking several PlayStation 3 hackers to court. PS3 "modder" George Hotz and Sony eventually settled out of court. But attacks on Sony continued, with a major breach at the PlayStation Network that exposed 77 million customer records and at Sony Online Entertainment where more than 24 million records were exposed. Sony has suggested connections between Anonymous and the breaches. While Anonymous was admittedly behind the initial DDoS, it says it wasn't behind the PSN and Sony Online Entertainment breaches, and hasn't claimed credit for any other Sony attacks. Last week, Spanish police arrested three people accused of taking part in Anonymous activities and Anonymous members retaliated by hitting the Spanish National Police Web site. This week, Turkish police arrested 32 people, including eight who were teens, within days of the group launching a campaign to shut down a Turkish government site in response to new Internet filtering laws. Yesterday, Anonymous was planning an attack on the site of the Federal Reserve for today.

Who is LulzSec?
Who's Behind the Hacks?

LulzSec first popped up in early May seemingly out of nowhere. But sources told CNET that the group is a spinoff from Anonymous ranks, but with no pretense of having a political message or moral principle. Indeed, the group's name, LulzSec--a derivative of LOL (laugh out loud) combined with security--is a strong indication that the group's motivation is to just hack for **kicks and entertainment**. The group makes a lot of jokes and taunts on Twitter and today said it would take hacking target requests. "Pick a target and we'll obliterate it. Nobody wants to mess with The Lulz Cannon - take aim for us, twitter."

**Who have they targeted?**

LulzSec began publicizing its hacking in May with the compromise of the Web site of the Fox TV show "X Factor" and exposed personal information of contestants, followed by release of internal Fox data. The group also has taken credit for hacks of Sony Music Japan, Sony Pictures, Sony BMG Belgium and Netherlands, Sony Computer Entertainment Developer Network (allegedly stealing source code) and Sony BMG, according to this timeline.

LulzSec hacked the **site of PBS.org** late last month, leaked passwords, and pasted a spoof news article on the site claiming that deceased rappers Tupac Shakur and Biggie Smalls were alive and residing in New Zealand. The group claimed they were punishing PBS for a Frontline program on WikiLeaks that they claimed was biased against the whistleblower site. LulzSec also has targeted Nintendo and the **Web site of FBI partner Infragard** in an attempt to embarrass the agency. LulzSec said it took the action against Infragard because of a plan by the Obama administration to classify cyberattacks as **acts of war**. Among the passwords on the Infragard site was one used by the CEO of botnet tracking firm Unveillance. The CEO told CNET that the hackers
used the password to read his e-mails and listen in on conference calls and that they threatened to extort money and botnet data from him. Botnets composed of compromised computers are typically used to send spam and to launch DDoS attacks. LulzSec recently went public with data stolen from a U.S. Senate Web site and released data stolen from the site of Bethesda Softworks, a subsidiary of gaming company ZeniMax Media. The group also recently compromised a site at the U.K. National Health Services. LulzSec did not release the information publicly, but sent an e-mail to the agency warning them about the problem and then released a redacted version of the e-mail to the public.

Who is Idahc?
Another hacker who has taken credit for attacking Sony is known as Idahc. He has identified himself as a 18-year-old Lebanese computer science student. In an interview this week with Andy Greenberg at Forbes, Idahc said he began hacking for "justice," then it became a game and now he's trying to prompt organizations to improve the security of their Web sites. "I don't hack for 'lulz' but for moral reasons," he said in the interview, adding that he considers groups like LulzSec to be "black hat," or criminal, hackers, and that he is a "gray hat" hacker.

Who has Idahc targeted?
Idahc claims to have stolen 2,000 records from Sony Ericcson's e-commerce site in Canada, leaked a database from Sony Europe, and compromised a Sony Portugal site. Meanwhile, there have been other copycat-type attacks on Sony, specifically a hacker with the alias "k4L0ng666" took credit for hacking Sony Music Indonesia and has reported a long list of other Web site defacements to cybercrime archive Zone-H. And someone with the handle "b4d_vipera" claimed responsibility for hacking Sony
Who's Behind the Hacks?

BMG Greece.

What about other big recent attacks? Are these all related?
In the past few months there have been a string of other computer hacking incidents, but they are not all linked. Unlike the Sony and other attacks conducted by Anonymous and LulzSec which were done to expose security weaknesses and embarrass a target and get publicity, other types of attacks are more malicious.

For instance, the networks of Citigroup and the International Monetary Fund were compromised recently. Reports have speculated that the IMF was targeted by a foreign government possibly wanting access to insider information that could affect financial markets. It's also unknown who is behind the Citigroup incident, although The New York Times reported that whoever did it managed to get in through the main customer Web site and then leapfrogged between different customers by inserting various account numbers into the browser address bar repeatedly. The data from accounts could be used for financial fraud, although the thieves apparently did not get card expiration dates or security codes, which will make the data more difficult to use.

Then RSA warned customers in March that its system had been compromised and data was stolen related to its SecurID two-factor authentication devices, which are widely used by U.S. government agencies, contractors, and banks to secure remote access to sensitive networks. Within a few months, reports trickled out about breaches at three defense contractors: Lockheed Martin, L-3 Communications, and Northrop Grumman, the first two of which confirmed that the attacks were related to SecurIDs. It's unclear who is behind the attacks, but when it comes to military espionage foreign governments or nation states are often suspected. In this case several experts
speculated it could be China.

**Google announced** earlier this month that it had thwarted an attack aimed at snooping on hundreds of Gmail accounts owned by U.S. and other government officials, journalists, and political activists that appeared to originate in China. Chinese representatives have denied any involvement.

There was also a breach at e-mail marketing service provider **Epsilon** in April that prompted big companies like Citibank, Chase, Capital One, Walgreens, Target, Best Buy, TiVo, TD Ameritrade, and Verizon to warn customers that their e-mail addresses had been exposed.

And **in March** someone stole digital certificates from registration authorities associated with Comodo and could have used them to spoof sites like Google, Yahoo, Live.com, and Skype. A 21-year-old Iranian patriot **claimed responsibility** for the attacks, saying he was protesting U.S. policy and was taking revenge for last year’s Stuxnet malware that **experts believe** was created to shut down Iran’s nuclear program.
Prepare for the 'Advanced Persistent Threat'

Prepare for the "Advanced Persistent Threat"

Security experts say companies need new tactics to fight the next wave of cyberattacks.

THURSDAY, JUNE 16, 2011
BY LAUREN COX

A recent string of cyberattacks against large companies, government contractors, financial institutions, and even security providers themselves has highlighted a new type of heist: the advanced persistent threat, or APT.

This spring, these ambitious attacks have hit organizations that have valuable data and the resources to defend it well, including Google, Citigroup, and the International Monetary Fund. A recent APT-style attack on RSA, which provides security technology to some of the biggest banks, alarmed RSA's high-profile clients and appears to have led to an intrusion at Lockheed Martin, an RSA customer.

Unlike recent website takeovers by brazen "hacktivists" or massive thefts of credit card data, APTs are elaborate and sustained con jobs that are difficult to detect. The term was coined by government organizations accustomed to fighting online espionage, says Tom Cross, manager of the IBM X-Force Advanced Research security team, but these kinds of attacks are now becoming common enough to be discussed in corporate boardrooms. In a March survey of 563 IT security specialists by nCircle, a security technology company, 16 percent of the respondents listed APTs as their biggest security concern in 2011. That made it the second-most-worried-about security issue; 26 percent of respondents said their top priority was complying with security-related regulations.

RSA did not respond to Technology Review's requests for interviews, but Uri Rivner, the company's head of consumer identity protection, described some details of the
Prepare for the 'Advanced Persistent Threat'

attack in a company blog. First, one employee, who had limited administrative access to internal files, fell for a phishing scam and opened a spreadsheet labeled "2011 Recruitment plan.xls." Rivner said the file exploited a zero-day (previously unknown) security hole in Adobe Flash software. The hackers then installed a remote administration tool and breached multiple employees' accounts before extracting information over FTP, or file transfer protocol. According to Rivner and Cross, the breach had many of hallmarks of advanced persistent threats: repeated attempts to find a weak human link, a zero-day opening, sophisticated malware, and strategic methods to avoid detection while extracting data. APTs may lie dormant for months before finding a strategic moment to extract information.

"The first thing that these people do is collect info about their target," Cross says. "We put a lot of information about ourselves—both our personal and work life—on the Internet, so it's easy to do research and develop a profile of an organization."

That's one reason why many security experts urge companies to assume they are going to be targeted. "That's the reality," says Catherine Lotrionte, executive director at the Institute for Law, Science and Global Security at Georgetown University. As a result, she advises companies: "Make sure you have the best intrusion detection in place."

When RSA was attacked, it was using the services of a company called NetWitness to detect unusual activity across its networks. NetWitness was in fact "instrumental" in detecting the intrusion, says Eddie Schwartz, who was that company's chief security officer and has held the same title at RSA since it recently acquired NetWitness. Schwartz declined to reveal details of how the company detected the intrusion. However, he says that overall, the idea of securing networks by trying to "build a gigantic wall that nobody can climb over" is outdated. Training all employees to better detect phishing won't significantly help, he says, essentially because there will always
be someone who will fall for a scam.

IBM's Cross disagrees; he thinks more companies should try training employees to be more alert for phishing or other signs of cyberattacks. "The goal is not to stop everything; the goal is to detect something," he says. "If you educate these people and show them that there is a real threat, they become your front line."
For Recent Cyber Attacks, Motivations Vary
by TOM GJELTEN

Listen to the Story

June 16, 2011

Computer users have for years struggled with viruses, worms and all sorts of malware. But the most recent cyberattacks have targeted institutions whose computer systems were thought to be relatively secure: the French Ministry of Finance, Sony, Lockheed Martin, Citibank, even the International Monetary Fund.

"These are first-class attacks," says Luis Gorrons, technical director for Panda Security, a global cybersecurity firm. "We were always seeing attacks on small and medium companies, but now we're seeing that many big companies are being targeted and successfully attacked."

It's a cyber barrage.

The people hacking into these big computer networks are for the most part highly sophisticated, with advanced tools and software at their disposal. But their motivations vary.

There are, for example, the "hacktivists" who break into networks largely just to disrupt them and make a political point. A recent penetration of the U.S. Senate computer system fit this pattern, as did an apparent attack Wednesday on the CIA's website.

There are also cybercriminals, seeking to commit fraud or raid bank or credit card accounts, as at Citibank or Sony.

Finally, there are the cyberspies who want to steal military secrets from a defense contractor like Lockheed Martin or financial data from the IMF.
If someone is breaching a defense contractor, it's probably at the behest of a foreign nation. If someone is breaching the IMF, it's probably at the behest of a foreign nation looking for competitive [intelligence] on what's going on.

- Anup Ghosh, CEO of cybersecurity firm Invincea

"If someone is breaching a defense contractor, it's probably at the behest of a foreign nation," says Anup Ghosh, chief executive of Invincea, a Virginia-based cybersecurity firm. "If someone is breaching the IMF, it's probably at the behest of a foreign nation looking for competitive [intelligence] on what's going on."

The IMF decides which governments deserve financial bailouts, under what conditions, and the fund's actions have enormous implications for the global economy.

"If I can jump into the pool of water that is the IMF system, I can not only read the minds of the central banking community, but I can also manipulate currency and bond markets around the world," says Tom Kellermann, chief technology officer at AirPatrol Corp.

A hacker penetrating the IMF system might know which country's currency is likely to rise or fall in value and which government debts are likely to get paid off and which aren't. He could learn what negotiating stance IMF officials might take with a member government.

Those are important secrets, but the IMF may have neglected the challenge of protecting them.

"For years, they have emphasized physical security," says Kellermann, who used to manage cybersecurity at the World Bank, the IMF's sister institution. "The most important thing was protecting the executives and the decision-makers and the conference rooms wherein they made serious global decisions that had implications for the global financial markets."
In the meantime, however, the expansion of information technology and the widening use of mobile devices and remote access to sensitive systems complicated the security challenge at institutions like the IMF.

"You're seeing hackers leapfrog through these remote access points into the inner sanctums of these institutions," Kellermann says, "and maintain this omniscient presence within the systems by which they can manipulate markets."

The data breach at the IMF remains under investigation, and it is not yet clear who might have been responsible for the cyberattack. Governments would probably have the greatest interest in IMF data and confidential information, but that does not necessarily mean the attack was carried out by a state actor.

"There are underground markets [for data]," Ghosh says. "What we're seeing today is widespread and indiscriminate looting of networks." The IMF breach, he says, fit this pattern. "The person who is gathering that data may try to sell it to the highest bidder," he says.
The Pentagon's advanced research arm tackles cyberspace

By Jim Wolf
WASHINGTON | Thu Jun 16, 2011 1:56pm EDT

(Reuters) - The Pentagon's advanced research arm, the same group credited with developing the forerunner of the Internet in the 1960s, is working on many fronts to boost U.S. defenses against computer-generated attacks.

The Defense Advanced Research Projects Agency, is building a virtual firing range in cyberspace -- a replica of the Internet on which scientists can test how successfully they can thwart feared foreign- or domestic-launched attempts to disrupt U.S. information networks.

Called the National Cyber Range, it will also help the U.S. government train cyberwarriors and hone advanced technologies to guard information systems.

Reuters has learned that the National Cyber Range is expected to be fully up and running by mid-2012, four years after the Pentagon approached contractors to build it. It cost an estimated $130 million.

One of these companies is Lockheed Martin Corp, the Pentagon's No. 1 supplier by sales and itself the target of what it called "a significant and tenacious" cyber attack last month.

Lockheed, the U.S. government's top information technology provider, was awarded a $30.8 million contract in January 2010 to continue to develop a prototype. Johns Hopkins University's Applied Physics Laboratory won a similar deal at that time.

This summer DARPA is to select one of them to operate a prototype test range during
Pentagon's Advanced Research Arm Tackles Cyberspace

a yearlong test.

It will also apparently help train cyberwarriors such as those in the U.S. military's Cyber Command, ordered up by Defense Secretary Robert Gates in June 2009 after he concluded the threat of digital warfare had outgrown existing U.S. defenses.

The cyber range actually will be a collection of "testbeds" that can carry out independent drills or be woven into one or more larger pieces, depending on the challenge.

The range is to test such things as new network protocols plus satellite and radio frequency communications.

A key goal is to run classified and unclassified experiments in quick succession, "in days rather than the weeks it currently takes," said Eric Mazzacone, a DARPA spokesman.

That would require a system capable of being completely reset after an experiment -- reconfiguring it and purging all data from related memory, hard drives and storage devices.

Such an ability to reboot and start over is central to the plan, keeping the facility available "at all times for both experimentation and training," without fear of corruption or compromise, Mazzacone said by email.

CRASH AND CINDER

DARPA is also working on other plans to advance cyber defense.

A program known as CRASH -- for Clean-slate design of Resilient, Adaptive, Secure Hosts -- seeks to design computer systems that evolve over time, making them harder for an attacker to target.
The Cyber Insider Threat program, or CINDER, would help monitor military networks for threats from within by improving detection of threatening behavior from people authorized to use them. The problem has loomed large since Army Private First Class Bradley Manning allegedly passed a trove of confidential State Department documents to WikiLeaks, the anti-secrecy website.

Then there is "Cyber Genome," aimed at automating the discovery, identification and characterization of malicious code, which could help figure out who was behind a cyber strike.

President Barack Obama has asked Congress for more than $250 million to fund DARPA's cyber initiatives in the coming year, double his fiscal 2011 request.

The U.S. Defense Department, meanwhile, is preparing an expanded pilot program to boost the sharing of cybersecurity information with the companies that provide arms, supplies and other services costing some $400 billion a year.

The new effort, like a predecessor that began in 2007, is voluntary and is aimed at protecting sensitive but unclassified information on or passing through computers owned by companies that make up what the Pentagon calls the defense industrial base, or DIB.

About 35 companies took part in the initial program, including Lockheed Martin, which said last month its computer networks had become "a frequent target of adversaries around the world."

The expanded "DIB Opt-In" program will be open to many more companies. It is "vital to the nation's military readiness and the government's overall efforts to enhance cybersecurity," Air Force Lieutenant Colonel April Cunningham, a Defense
Department spokeswoman, said in a statement to Reuters.

Ultimately, the new program may be a step toward putting major Pentagon contractors behind military-grade network perimeter defenses, such as those that protect the Pentagon's own classified networks.

(Reporting by Jim Wolf; Editing by Jackie Frank)
Hackers Declare War on Government Agencies

June 20, 2011, 4:55 PM
Hackers Declare War on Government Agencies
By NICK BILTON

The Internet may be about to get a little more chaotic than usual. Over the weekend, a group of hackers declared that they are initiating cyber warfare with governments and security companies around the world.

The group, Lulz Security, has claimed responsibility for a number of recent data breaches and have already attacked a number of United States government and corporate Web sites. Lulz Security also said it was working closely with another group called Anonymous, a loosely affiliated team of activist computer hackers. Although Anonymous did not put out its own statement about the attacks, the two groups have been communicating regularly on Twitter.

In a letter posted on a public Web site, Lulz Security announced its plan to attack more government sites and encouraged other groups and individuals “to open fire on any government or agency that crosses their path.” The undertaking is called “Operation Anti-Security.”

“Top priority is to steal and leak any classified government information, including email spools and documentation,” Lulz Security wrote in the letter. “Prime targets are banks and other high-ranking establishments.”

The Federal Bureau of Investigation declined to comment on the letter.

Last week Lulz Security breached the Web server of the United States Senate and briefly brought down the Central Intelligence Agency Web site through a denial-of-service attack. The group has also been responsible for attacks on Sony, Bethesda Softworks, a gaming company, and a string of other sites.
Kindergarten-Level Computer Security

How Citigroup let itself fall prey to an easy hack.
By Kenrick Vezina

If you've ever been exploring the Web and manually altered part of the URL in your browser's address bar—say, to access a different folder on Flickr, or a different friend's profile on Facebook—you've performed the simple technique that hackers recently used to compromise more than 360,000 bank accounts from Citigroup.

This spring, according to the New York Times, hackers with legitimate Citi credit card accounts logged in to the website and noticed that the URLs displayed data unique to each account. By changing a few digits in the URL, the hackers found themselves inside other people's accounts without ever having to log in as those people. From there, they used custom software to automatically substitute account numbers, enabling them to access many accounts in a short time, the Times reported. (Citigroup declined to comment beyond a statement acknowledging that the hackers obtained names, account numbers, e-mail addresses, and transaction histories.)

Bruce Schneier, chief technologist for the telecommunications company BT, says that preventing the URL from displaying account-specific information is "kindergarten security." Security researcher L. Jean Camp of Indiana University agrees that the hack was remarkably simple. "Can you believe it?" she says.

Which raises a question: How could a sophisticated financial institution—one that has been hacked before—let something like this happen? Essentially, it built a vault of solid steel and used balsa wood for the door.

Balkanization inside Citigroup may have played a part. Large organizations, Camp says, usually have separate groups for customer service and network security. In a typical company, employees know that certain tasks must always go through certain departments—all personnel changes through Human Resources, for instance. But such a "gatekeeping" role does not always exist for security. This means that a customer service group might design a Web page for credit card holders without necessarily running it past security first. Camp has consulted with at least one major company in which the user interface team said, regarding its design, "If we add security, we'll break it." Security is usually called in only in response to a threat or breach, Camp notes.

And even if a company pays close attention to security, the complexity of the
organization can trip it up, says Patrick Peterson, a security expert at Cisco Systems. He points out that other parts of Citigroup apparently had addressed this same security hole, even though the credit card group did not. The company "might have 20, 30, 40 lines of business," he notes, "and 99.999 percent of the time they get it right. Then someone forgets something. It doesn't make it okay, but it is difficult to scale things forever."

Chris Novak, managing principal of Verizon's security branch, which consults with businesses about intrusion prevention, says security oversights often result from an us-or-them approach. In other words, many organizations assume that employees and other insiders can be trusted, so they focus on defending against outside threats. But in designing their systems with these two groups in mind, they often overlook a third group: those who are "not an unknown but not an employee." That's essentially what happened in the Citi heist, when the hackers were never faced with the defenses meant for complete outsiders. It's as if the company assumed that bank robbers don't have bank accounts.

Novak says that when organizations are shown the vulnerabilities these users-but-not-employees can exploit, their first response is usually, "Well, why would a user do that?" Furthermore, he adds, a lot of large organizations "have a mind-set that they don't have small problems." They end up worried about "Mission: Impossible situations," he says, but the vast majority of attacks are "opportunistic."

Schneier suggests a more calculating explanation for Citi's lack of proper defenses. Maybe the bank didn't spend the money on good security because it figured that it would be cheaper and simpler to reimburse its customers for any fraudulent charges, he says.

Whatever the reason, these basic security weaknesses are more common than you might expect, Novak says. Faults similar to Citigroup's show up each year in Verizon's Data Breach Investigation Report, an analysis of hundreds of intrusions. In the 2011 report, for instance, only 18 percent of the cases Verizon investigated resulted from hacks of "high" difficulty—requiring "advanced skills."

Copyright Technology Review 2011.
HOOGEZAND-SAPPEMEER, Netherlands—In this sleepy Dutch town last December, police burst into the bedroom of 19-year-old Martijn Gonlag as he hurriedly pulled on jeans over his boxer shorts. He was hauled away on suspicion of taking part in cyber attacks by the online group calling itself Anonymous.

Mr. Gonlag admits taking part in several attacks on websites, but he recently had a change of heart as some hackers adopted increasingly aggressive tactics.

History of 'Anonymous'

"People are starting to grow tired of" the hackers, he said in an interview. "People are also starting to realize that Anonymous is a loose cannon."

Now he appears to be a target himself. A chat room he hosts faces frequent hack attacks, he says.

Mr. Gonlag’s role reversal provides a glimpse of the unruly hunt-or-be-hunted world underpinning a string of online attacks against major companies and government bodies—incidents that have sparked a digital manhunt by law-enforcement agencies in several countries.

What once was just righteous rabble-rousing by Anonymous in the name of Internet freedom has mutated into more menacing attacks, including by a splinter group of Anonymous called LulzSec, which is alleged to have moved beyond paralyzing websites to breaking in to steal data.

The tumult over online agitators like Anonymous comes at a time when the world’s computers are under unprecedented attack. Governments suspect each other of mounting cyber espionage and attacks on power grids and other infrastructure. Criminal gangs using sophisticated viruses cull credit-card and other sensitive data to
Now "hacktivists" who populate groups like Anonymous and LulzSec, mostly young males from their teens to early 30s, have also ignited increasing concern among computer experts over the security of corporate and government systems.

Authorities in the U.K., Netherlands, Spain and Turkey have made more than 40 arrests of alleged Anonymous participants. In the U.S., the Federal Bureau of Investigation has conducted sweeping searches as part of a continuing probe into various attacks. On Wednesday, U.K. police charged a 19-year-old believed to have ties with both Anonymous and LulzSec, a group whose name is a blend of "lulz," or laughs, and "security."

Anonymous and LulzSec pose a problem for law enforcement partly because their membership and operations are difficult to pin down. They are amorphous entities with scant leadership structure or formal process for making decisions.

Anonymous is "an idea" rather than a group, said Gregg Housh, a 34-year-old Web designer from Boston. "There is no one group, no one website. That is what makes it so powerful in my eyes." Mr. Housh said he helps Anonymous with logistics but doesn't take part in attempts to shut down websites or do anything illegal.

Waves of infighting spring up periodically within Anonymous, Mr. Housh added. "This is very natural. It's what happens."

A watershed in its tactics came in February when it hacked a California-based Internet-security firm called HB Gary Federal LLC, which sells investigative services to companies and government agencies, and released tens of thousands of internal emails.

**Types of attacks by Anonymous or LulzSec:**

**Denial-of-service attacks**

Computer users bombard website servers with data in the hopes of knocking them offline. Among targets have been companies, such as PayPal and MasterCard, as well as government sites, including the CIA's. Such attacks can cost tens of thousands of dollars for the victim, including the cost of defending against the attacks and improving
security.

**Hacking**

Break-ins into computer systems, potentially giving access to sensitive data such as customer information and internal emails. A hack into Sony's systems resulted in the theft of personal data of about 100 million online video-game users. Sony shut its popular PlayStation online network for nearly a month, and has estimated the attack cost it about $171 million. Anonymous participants said the group didn't orchestrate the attack, but couldn't rule out that someone involved in the group could be involved.

**Doxing**

Involves finding personal information about people and disclosing it online. LulzSec this week claimed to rat out two U.S. individuals it said had "tried to snitch" on the group, apparently disclosing names, addresses and other contact information.

The incident sent a chill through the security industry. "Computer-security specialists are afraid to challenge Anonymous," said Mikko Hypponen, of computer-security firm F-Secure Corp. "No one is that confident in their own systems."

Some participants involved in that hack formed the LulzSec splinter group, according to security specialists and participants. LulzSec has claimed credit for a string of computer break-ins, intensifying the response from law-enforcement groups.

Anonymous grew out of an online message forum formed in 2003 called 4chan, a destination for hackers and game players fond of mischievous pranks. Its followers became more politically focused, embracing an ideology of Internet freedom. In 2008, it made headlines with a campaign against the Church of Scientology, protesting what Anonymous claimed was the religious group's effort to control information about itself online.

The campaign included "denial-of-service" attacks—bombarding websites with data to try to knock them offline. Later attacks targeted the movie and music industries, because of their efforts to stop piracy.

In December, the group hit on a cause that propelled it into the spotlight: WikiLeaks. Anonymous began attacking organizations and people who tangled with WikiLeaks and founder Julian Assange, who had been arrested in London over sexual-misconduct
allegations in Sweden, which he denies.

Anonymous attacks shut or slowed websites of businesses that had cut ties with WikiLeaks, including MasterCard Inc., Visa Inc. and PayPal, a unit of eBay Inc. All said their systems weren't compromised. PayPal said the attacks temporarily slowed payments via its website but not significantly.

People wore masks of the online group Anonymous and of WikiLeaks's Julian Assange (at right) at a demonstration in Spain in December.

The campaign, Operation Payback, brought Anonymous new followers from around the world. Via online chat forums and social-media websites, participants disseminated instructions about how to download attack software and about sites to target. Software called LOIC, or low-orbit ion canon, was downloaded tens of thousands of times, security specialists say.

Among recruits was Mr. Gonlag, under the nickname Awinee, an online handle the Dutch youth had used during a lifetime of intensive video-game playing. Spurred by talk of the WikiLeaks campaign in chat rooms, he piled in, at one point writing: "Fire, fire fire."

Mr. Gonlag has admitted he participated in attacks including one against the website of a Dutch prosecutor who announced the arrest of a 16-year-old in connection with the WikiLeaks campaign.

Returning home in the early hours of Dec. 10, Mr. Gonlag said in an interview, he typed
Inside the Anonymous Army of 'Hacktivist' Attackers

the address of the prosecutor's website into the attack software and let his computer fire data for about half an hour. That afternoon, Dutch police arrested him and seized his desktop computer and phone.

Mr. Gonlag, who awaits trial, is charged with crimes related to destroying a computer network and inciting others to cause an attack, which carry a possible six years in prison.

Tapping at his keyboard recently in jeans and a green T-shirt, Mr. Gonlag said that he took part in several pro-WikiLeaks attacks, which he likened to a "digital sit-in," but that he wasn't guilty of the charges because he didn't destroy or steal anything.

He indicated he grew disenchanted as some arms of Anonymous allegedly moved from paralyzing websites to stealing from them, putting the group in "a very, very bad position."

Alluding to the cyber attacks he himself now faces, he said that when his computer server that powers the online chat rooms comes under fire, he takes the server offline and waits until his attackers tire of the effort. Then he connects back online again.

Each online Anonymous forum, such as AnonOps and AnonNet, has multiple chat rooms or "channels," typically focused on a particular operation or theme.

While there may be a hundred or so active followers of a network on a regular basis, numbers swell into the thousands during popular campaigns.

Many channels are public, but participants can also set up invitation-only chat rooms or send each other private messages. Participants often speak online using audio or camera software, and they also can share videos and other files. Many participants are U.S.-based but there is also a significant following in Europe and elsewhere.

Discussion ranges from political theory to technical chatter to juvenile banter. In one chat log, a participant promised to push a company "so far into orbit that they'll transmute into a gravitational dip and exude Hawking radiation."
Anonymous does have a hierarchy of sorts, with a core group of about 15 leaders who run the online chat rooms, participants say. They can issue sanctions, including banning someone from a channel or an entire network.

"There are nodes of power and authority, but it is pretty decentralized, and no one is calling the shots for all the operations," said Gabriella Coleman, a New York University academic who follows Anonymous.

The Anonymous attacks turned more ominous in February, when some members broke into HB Gary Federal's systems.

The Internet-security company's then-chief executive, Aaron Barr, noticed the problem one morning when he was unable to access corporate email via an iPhone.

He instantly suspected Anonymous, as he had been quoted in a newspaper article saying he had uncovered key participants. Soon, his Twitter account was hijacked and used to post racial slurs and his Social Security number. Then Anonymous announced it had hacked his email and would make the contents public.

"I was shocked and consumed by it," Mr. Barr said.

By hacking into the company's public Web page and stealing passwords, attack participants obtained about 70,000 emails, which they posted online. The traffic included details of a proposed effort to gather information on critics of the U.S. Chamber of Commerce in an attempt to prove illegal activity by labor-union members. Mr. Barr said the initiative was only intended to show what information could be retrieved.

The attackers also exposed minutiae of Mr. Barr's marital issues. He said the personal communications were taken out of context.

Mr. Barr stepped down from his job in late February.

Anonymous participants say the attacks expose weaknesses in the systems of computer-
security companies and large organizations. "They should be scared," said Corey Barnhill, a 23-year-old New Jersey native who uses the online nickname Xyrix and who said he took part in the attack on HB Gary Federal. "You're college-educated and you can't secure a server? How hard is it? They can't keep a kid out?"

Mr. Barnhill said the HB Gary Federal hack was designed to teach Mr. Barr a lesson for suggesting he could unmask Anonymous. "Whacking him down a peg was pretty funny," he said.

In April, an Anonymous denial-of-service attack against Sony Corp. was followed by a breach of its computer system that resulted in the theft of names and birth dates and other personal information on about 100 million people who play online video games through Sony's online gaming services.

Sony shut down its PlayStation online network for nearly a month and has estimated the attack cost it $171 million, including costs for enhanced security.

Sony has said that it isn't clear that any credit-card data were ever accessed. The company said it has added security to its systems.

Sony told U.S. lawmakers it found a file left on its servers called "Anonymous," the contents of which said "We are Legion," a tagline often used by Anonymous.

Anonymous participants claim responsibility for the denial-of-service attacks, in press releases and via their Twitter account. They said the group didn't orchestrate the data breach but didn't rule out that someone from the group could have been involved. Meanwhile, the LulzSec group formed.

Security experts who follow LulzSec say it has about 10 core participants and is known for its hacking expertise. In recent weeks it has claimed responsibility for breaking into computer systems of several organizations, including the U.S. Senate and an FBI affiliate called InfraGard.

Last week, LulzSec said it had knocked the Central Intelligence Agency's website offline.
Inside the Anonymous Army of 'Hacktivist' Attackers

for about an hour. The CIA said no internal or classified networks were affected.

A call to a phone number set up by the group, 614-LULZSEC, wasn't returned. One LulzSec follower called "tflow" responded to a Wall Street Journal reporter in an online chat room, saying: "Unfortunately the gnomes are too busy to pick up your clearly inferior call."

"For the past month and a bit, we've been causing mayhem and chaos throughout the Internet, attacking several targets," LulzSec said in a statement last week. "This is the Internet, where we screw each other over for a jolt of satisfaction."

This week, LulzSec claimed to rat out a couple of individuals it said had "tried to snitch" on it. In a document addressed to the "FBI & other law enforcement clowns," the group appeared to reveal the full names, addresses and other contact information of two U.S. men it claims were involved in some hacks. "These goons begged us for mercy after they apologized to us all night for leaking some of our affiliates' logs," according to the document, accessed via a link on LulzSec's twitter page. "There is no mercy on the Lulz Boat."

—Ian Sherr contributed to this article.

Read more: http://online.wsj.com/article/SB10001424052702304887904576399871831156018.html#ixzz1Q6RbLrxB
For weeks now, tech headlines have been dominated by news of security breaches, data dumps, and hackers. It kicked off in April when Sony had to take its PlayStation Network offline for nearly a month after a massive hack, but has since moved to focus on the vocal and unapologetic LulzSec.

But who are these people? What do they want? Can they be stopped, or are we one hack away from having all our personal information posted on Twitter, Pastebin, or The Pirate Bay?

The two groups making the most headlines are LulzSec and Anonymous. LulzSec has gained in popularity in recent months, but Anonymous has been around for several years. In general, Anonymous organizes distributed denial of service (DDoS) attacks against political targets—government with which they do not agree or companies, like Sony, filing lawsuits against hackers. LulzSec has also targeted government sites—like the CIA and Senate.gov—but the group has also hacked gaming companies and published the personal information of average Web users just for kicks, or lulz.

Recently, LulzSec and Anonymous teamed up for a project known as Operation Anti-Security, in which they pledged to target the Web sites of government agencies via DDoS attacks or defacement. But despite the cooperation, both groups still have their own agendas. Let's take a look.

**ANONYMOUS**

Anonymous has been around for years, but really picked up steam and garnered national attention in 2008 when it went after the Church of Scientology. At the time, a video of actor Tom Cruise speaking about Scientology ended up on YouTube, and the church demanded that it be removed. Media sites like Gawker, however, kept it up. "It's newsworthy; and we will not be removing it," Gawker's Nick Denton wrote.

Anonymous viewed the church's efforts to wipe the videos as Internet censorship. In a 2008 YouTube video, the group pledged to "expel you from the Internet and systematically dismantle the Church of Scientology in its present form." The campaign became known as Project Chanology (Anonymous reportedly includes members of the "/b/" bulletin board 4chan.org) and included various hacks, protests, and pranks, prompting the church to accuse Anonymous of religious hate crimes.

In the years that followed, Anonymous targeted a number of groups with which it did not agree, like the Westboro Baptist Church. More recently, the group made headlines
for going after security firm HBGary Federal, companies that cut ties with Wikileaks, and Sony.

Anonymous attacked HBGary's site on February 6, days after CEO Aaron Barr told the *Financial Times* that he knew and planned to expose the identities of leaders behind the Anonymous collective. The cyber attack resulted in the defacing of Barr's online networking profiles and exposure of 71,800 e-mails at AnonLeaks. The controversy prompted Barr to resign his post.

The Wikileaks saga started after the whistleblower site published about 250,000 State Department cables. Soon after, companies like MasterCard, Visa, and PayPal stopped processing donation payments, while Amazon refused to host the site. Anonymous accused the companies of bowing to government pressure and organized DDoS attacks against the sites, taking them down or slowing them significantly. That prompted Twitter to temporarily suspend the group's feed.

Sony, meanwhile, felt the wrath of Anonymous after it went after those who hacked its PlayStation 3, most notably George "Geohot" Hotz. In April, Anonymous attacked Sony-branded Web sites to protest Sony's lawsuits. An Anonymous offshoot known as "SonyRecon" also targeted individual Sony employees.

When Sony's PlayStation Network was hacked in April, Anonymous denied any involvement. But Sony said it uncovered a file on a Sony Online Entertainment server that said "Anonymous." A group spokesman said Anonymous was being set up, but the decentralized nature of the group made it hard to know who was telling the truth. Essentially, if you say you're a member of Anonymous, you're a member of Anonymous so a member could have done it without the higher ups knowing.

It hasn't been completely smooth sailing for Anonymous members. Earlier this month, police in Spain and Turkey arrested members of the group for alleged DDoS attacks. Officials in the UK also arrested Anonymous members back in January, while FBI officials here executed search warrants. Anonymous said officials made a "sad mistake" and vowed revenge.

As a result, much of Anonymous' activity lately has been targeting governments that arrest its members, like Spain, or those with Internet policies that Anonymous deems oppressive, like Syria. The group also launched a campaign against Federal Reserve chairman Ben Bernanke because it felt the U.S. government has failed its citizens.

Given the attention LulzSec has received, however, it made sense that Anonymous teamed up with the group for an project dubbed Operation Anti-Security.

"The government has tried to take control of our Internet ocean," Anonymous said in a recent [YouTube video]. "We are sending our fleet to fight alongside the lulzboat to
LulzSec? Anonymous? Know Your Hackers

reclaim what is rightfully the peoples’. It's time to show the corrupt governments of the world that they have no right to censor what they do not own."

**Communication:** There are a variety of Anonymous-related Twitter feeds, but lately, most of the news is coming from @AnonOps. The group also has a blog at anonops.blogspot.com and youranonnews.tumblr.com and a Facebook page. Barrett Brown is also considered a sometimes spokesman for Anonymous, and he tweets via @BarrettBrownLOL.

**Major Targets:** Church of Scientology, HBGary Federal, anti-Wikileaks sites, Sony, Web sites of governments that censor the Internet.

**Symbol:** Anonymous has adopted the Guy Fawkes mask used by the title character in the "V for Vendetta" graphic novel series as its symbol.

**Catchphrase:** We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.

**LULZSEC**

LulzSec emerged in the past few months, but has quickly wrestled the headlines away from Anonymous, perhaps due to the juvenile and taunting nature of many of its tweets. Everyone is a target and very few things are off limits; at one point, the group opened up a hotline where it took hacking requests.

LulzSec first got noticed, however, when it hacked the Web sites of Fox.com and PBS. It stole Fox employee passwords and posted them online and took over the Twitter account of a Fox affiliate.

Weeks later, in response to a Frontline special about Wikileaks it did not like, LulzSec targeted PBS, posting a fake news story that said deceased rapper Tupac Shakur was still alive.

The group soon took to Twitter to spread its message via @LulzSec; the feed now has almost 250,000 followers. LulzSec has used the micro-blogging site to announce its next targets, post links to data it has stolen through various hacks, and taunt its enemies. Twitter did not respond to a request for comment about whether LulzSec's activities violates the company's terms.

Given that the Twitter feed is the group's main source of communication, however, perhaps law enforcement wants them to remain online so their activities can be monitored. Since the PBS and Fox.com hacks, LulzSec has also targeted
LulzSec? Anonymous? Know Your Hackers

SonyPictures.com, FBI affiliated Web sites, Nintendo, Bethesda Softworks and other small gaming companies, Senate.gov, and the CIA, among others.

Ostensibly, LulzSec is calling attention to the lackluster security practices used by the companies that house our personal data. But major corporations have not been the group's only targets. Recently, LulzSec released the emails and passwords of 62,000 average Web users, people who subsequently had their emails hacked, Facebook accounts defaced, and Amazon accounts charged. After playing with the aforementioned hacker hotline for awhile, meanwhile, LulzSec started redirecting its number to legitimate companies, like the World of Warcraft hotline.

In honor of its 1,000th tweet, LulzSec last week posted an admittedly pretentious manifesto of sorts, in which it admitted to "causing mayhem and chaos throughout the Internet."

But there are far more nefarious characters than LulzSec currently having their way with your data, the group argued. "Do you think every hacker announces everything they've hacked? We certainly haven't, and we're damn sure others are playing the silent game," LulzSec wrote. "This is what you should be fearful of, not us releasing things publicly, but the fact that someone hasn't released something publicly."

Still, in discussing its accountability, LulzSec said simply that "this is the lulz lizard era, where we do things because we find it entertaining."

Yesterday, however, LulzSec insisted that it's not all fun and games. "To all the eager and intelligent press, our tweets are lighthearted, but the work is ongoing hard. We have a lot of data to sift through," it tweeted.

On Tuesday, UK police arrested a 19-year-old suspected of masterminding recent hacks, leading some to believe he was the face of LulzSec. The group, however, denied any direct affiliation, arguing that LulzSec was, at best, "mildly associated" with the teen, who was identified as Anonymous antagonist Ryan Cleary.

**Communication:** The majority of LulzSec's messages are sent via Twitter @LulzSec, though it also has a Web site at LulzSecurity.com. Recently, a Brazilian arm of the group popped up at @LulzSecBrazil.

**Major Targets:** Fox.com, PBS, Sony Pictures, Nintendo, FBI, CIA, Senate.gov, small gaming firms.

**Symbol:** The group's Twitter feed image features a stick figure holding a wine glass and sporting a moustache, top hat, and monocle.

**Catchphrase:** The group frequently refers to executing hacks "for the lulz," urging
people to join the lulz boat and referring to its activities as lulz lizardry.

WHAT'S NEXT?

Neither group shows any signs of slowing down, and news of new hacks or targets emerges every day. Is there anything you can do to protect yourself? For the most part, Anonymous has targeted government sites and has not focused much on stealing and posting the confidential data of the average Web user. The same can't be said for LulzSec.

But as LulzSec points out, much of the trouble stems from the fact that people tend to use the same password across multiple sites, whether they're signing up for a newsletter or paying their credit card bill. If anything, these hacks should teach people to have multiple passwords for email, banking, credit cards, and online shopping. It can be difficult to remember multiple passwords, but it's better than having a LulzSec supporter hack into your Facebook account and change your photo to something obscene.

Also, many hackers will use your data to send phishing emails, in the hopes that you'll click on links and enter even more personal data. If you get an email that seems like it's from a legit source, like your bank or credit card company, don't click on any links. A company is never going to contact you and ask you to confirm your data via a Web form. If you get a phishing email, delete it; if you click on a link by accident, contact the company the message purported to represent to make sure there's no suspicious of fraudulent activity on your account.
No Easy Answers to Password Problems

Even "strong" passwords have big weaknesses, so companies serious about security ought to rely on additional methods of authentication.

- WEDNESDAY, JUNE 22, 2011
- BY ROBERT LEMOS

**Easier guessing:** Security researcher Troy Hunt analyzed 37,000 of the passwords stolen from Sony and found that half used only one type of character. This pie chart shows which category those weak passwords fell into: ones with only capital letters, ones with only lowercase letters, and ones with only numbers.
No Easy Answers to Password Problems

Credit: Troy Hunt

When hackers breached the servers of Sony Pictures in June, they cast a harsh light on one of the Web's most bedeviling security problems: passwords. After finding that 1 million user passwords for three Sony sites were stored without encryption, the intruders posted them online for anyone to see.

Security researcher Troy Hunt pored over the file and found that half of the passwords could be considered weak because they had a low degree of randomness—they had only lowercase letters, only uppercase letters or only numbers. More than a third of the passwords could have been found in a dictionary and easily guessed by a password cracker, a tool that quickly tries different combinations of secret words. Half of the passwords were seven characters or less. Finally, the researcher found 90 e-mail accounts that had also shown up in another leaked password file, from Gawker.com, and discovered that about two-thirds of those users had the same password at both sites. "It indicates to me that this was a normal practice for people to plug in the same password into their accounts," says Hunt, a software architect who studies security.

The Internet relies on passwords, and each person typically has dozens of accounts that require them. But as the Sony and Gawker episodes revealed, people often use passwords that are easy to guess or crack, and then repeat them across multiple sites. Better that than trying to remember dozens of complex strings of characters. And yet researchers who study passwords are just as lost as well.

"I truly wish I there was a simple prescriptive, constructive, bullet-point list of two or three things that users could do," says Cormac Herley, a computer scientist with Microsoft Research. "Unfortunately, I don't think I or anyone else has that list right now. So much of the last 10 years, so many people in security have been assuming that passwords would be gone. But more and more time has gone by, that has not
happened."

Instead, password-protected accounts have proliferated. Software for password management could be a solution, but relying on such an application has its own downsides. An attacker who infects a victim's PC gets the ultimate prize: the password for every account a user owns.

The situation looks worse when you consider that even our understanding of strong versus weak passwords might have flaws. In a recent paper, researchers from Florida State University, Redjack and Cisco Systems found that a typical measure of password strength—how much the chosen characters exhibit randomness or entropy—does not have a great deal of meaning. Password crackers follow certain strategies, first searching through certain dictionary terms, appending numbers to the guesses and then combinations of words. The researchers found that the cracking tools used by cybercriminals are generally very good at guessing a small but significant fraction of passwords—up to 20 percent for passwords of seven characters or more in about 10,000 guesses.
No Easy Answers to Password Problems

It’s familiar: This chart shows the 25 most commonly used passwords in the set of 37,000 that were analyzed by Troy Hunt and the number of times each one appeared.
Credit: Troy Hunt

The researchers argue that analyzing passwords for their level of entropy overestimates how easily hackers can crack some passwords and underestimates it for others, depending on how much time an attacker is willing to spend on the assault. As a result, says researcher Matt Weir, one of the authors of the paper, an organization that analyzes its passwords for randomness might have "an overly optimistic view of the security provided by their password creation policies."

It also means that forcing employees to change their passwords every so often might
not solve any meaningful problem. Instead, it may make it more likely that employees will reuse a password across multiple sites, meaning a hack on one can endanger accounts elsewhere. And although corporate networks and consumer Web services often lock out attackers who try multiple passwords in succession, hackers don't encounter such limitations if they gain internal access to the file where user passwords are cryptographically "hashed" before being stored. In that case, the password cracker can keep trying hashed versions of guesses at passwords.

Because of such flaws, security researchers say companies serious about security should not rely on just passwords. Using devices or software that generate one-time passwords, for example, forces an attacker to either steal the device or execute a real-time operation, known as a man-in-the-middle attack, in which the attacker modifies the connection between a victim and a service provider during a transaction. Such attacks are not unheard of—criminals have used banking Trojans, such as Zeus, to steal millions of dollars from small businesses and organizations using just such techniques—but the technology requires attackers to expect significantly more effort. "It is a more expensive attack," says Microsoft's Herley.
People imagine that sophisticated hacking requires sophisticated computers. The truth is that almost everything a hacker does can be done with a cheap notebook computer, or even a mobile phone.

The major exception is password cracking, and related crypto tasks like bitcoin mining and certificate forgery. In these cases, a minor investment in hardware can be warranted.

In particular, those who need to crack passwords (pen-testers, sysadmins, hackers) should buy a gaming graphics card in order to speed up cracking. Or, when buying notebooks for pen-testing, they should choose those with graphics processors.

What’s a GPU
Password Cracking, Mining, and GPUs

Computers, as we know them, used to contain a single processor, called the central processing unit or CPU”.

Now they contain a second processor, called the graphics processing unit or GPU. As the name implies, GPUs are intended for graphics, which means games and video.

But GPUs aren’t just for graphics; they are good for any highly repetitive task. Typical GPU applications include video transcoding, statistical modeling, physics simulations, medical imaging, financial modeling, and cryptography. Password cracking is just one form of cryptography.

It’s important to keep in mind that graphics processors are no more powerful than central processors. Trying to run non-repetitive tasks on the graphics processor results in a speed decrease. Foolish hackers regularly attempt this, and are regularly disappointed. Instead, graphics processors are optimized for calculations that are highly repetitive, whereas normal processors are optimized for the major of code that isn’t very repetitive.

These days, most computers come with a GPU. The iPhone has an ARM CPU and a PowerVR GPU. The latest Intel "Sandy Bridge" CPUs come with a custom Intel GPU built into the chip. AMD processors (formerly called "Athlon") have a version of the Radeon GPU on the chip. Except for AMD’s built-in GPUs, these aren’t programmable by the user, and therefore, can’t be used for anything other than graphics (although Intel keeps promising to make their GPU more programmable). Even AMD’s built-in GPU is slow relative to add-on GPUs.

Instead, when this paper mentions GPUs, it refers to the gaming cards with the fastest GPUs. Such cards can easily accelerate password cracking by 20 times. Using such cards, people are putting 8 GPUs in a system, accelerating password cracking by 160 times. That means a password that would otherwise take 6 months to crack can now be cracked in a day — assuming you are willing to spend $3000 on graphics cards.

Radeons are better than GeForce

There are only two manufacturers of high-end gaming cards: nVidia with their GeForce
Password Cracking, Mining, and GPUs

cards, and AMD with their Radeon cards. Both sell a wide range of cards, from the very cheap (but slow) to the very expensive (but fast). Prices typically range from around $100 for the cheaper ones, to $800 for the most expensive, with the best price-performance ratio around the $250 mark (two $250 cards will likely be faster than a single $700 card).

For gaming, Radeons and GeForces have roughly the same performance, with the fastest GeForce cards being the slight favorite. For super computer applications, like weather modeling or physics simulations, the GeForce cards are the clear favorite. However, for crypto, it’s the Radeon cards that come out on top. For equivalently priced cards, a Radeon card will be over twice as fast as a GeForce card when cracking passwords.

There are a few reasons for this. Radeons have twice the theoretical computer power when handling the "integer" numbers used in cryptography. Password cracking is able to tap into this theoretical power whereas most other applications (especially those using "floating point") cannot. In addition, Radeons have specific integer instructions like "bitalign" (aka. "rotate") and "BFI_INT" that speed up popular crypto operations.

Thus, a cheap model of the Radeon like the HD 5770 costing $109 will outperform an expensive GeForce model like the GTX 590 costing $749. The most expensive Radeon model, the HD 6990 costing $739, will be over three times as fast at cracking passwords.

Thus, the consequence is that if you want to crack WiFi WPA2 passwords, Windows NTLM password, Unix salted MD5 hashes, or Bitcoin hashes, then you should probably invested in one of these GPUs. Even a cheap $100 card can increase speed over your desktop processor by 20 times. Ideally, you should buy a Radeon card for this rather than a GeForce card.

Moore’s Law
Password Cracking, Mining, and GPUs

The above discussion applies to June 2011. Next year, CPUs and GPUs will be twice as fast.

But it's the *relative* performance that matters. Next year's $250 graphics card will likely outperform next year's CPU by 20 times. Unless AMD or nVidia makes radical changes to their chip architectures, the next generation of the Radeon will still likely outperform the next generation of GeForce cards.

Therefore, when you finally get around to buying that graphics card for password
cracking, you’ll have to look on the web for password cracking benchmarks to see which card is currently giving the best price/performance ratio.

**Notebook GPUs**

The above discussion have been for desktop computers that consume a lot of electricity. Pen-testers often don’t have that luxury -- they often only have a notebook (running something like BackTrack Linux). In that case, they want to buy a "mobile" version of the Radeon or GeForce chips. They can’t buy such chips as addons, but instead, have to choose a notebook that has their desired chip.

According to recent benchmarks, mobile Radeons are still faster than GeForces, but it’s highly variable. Notebook GPUs have an enormous range, as battery life is traded for gaming speed. Thus, one notebook with a powerhungry GeForce may be a better choice than another notebook with a battery conserving Radeon. You’ll have to look at benchmarks, or theoretical numbers (based on clock speeds and core counts) to figure
Password Cracking, Mining, and GPUs

out which is best for your needs.

Also note that there are three classes of laptops: the normal laptops, the low end
netbooks, and the high-end gaming laptops. Historically, only the high-end gaming
laptops contained graphics processors, but now graphics processors are appearing
throughout a wider range.

High-end gaming laptops are the best choice for password cracking power. The biggest
ones have graphics processors that rival desktop cards. You can buy an Alienware M18x
with a Radeon mobile GPU that is faster than all but the fastest desktop GPU. It’s also
18-inches across, weighs 8 pounds, lasts only a few minutes on battery, and costs $2400.

GPUs are becoming more popular in average notebook computers. Asus makes some
nice, average sized laptops with GeForce GPUs for a good price. Of particular note are
the current MacBook Pros (15 inch or 17 inch) which come with a good Radeon GPU. The
GPU is far slower than desktop GPUs, but of course, they don’t drain the battery, and
don’t jack up the price. My MacBook Air has a GeForce GT320M that triples password
cracking speed over the built-in processor (benchmarks below).

Curiously, GPUs are becoming popular for cheap "netbook" computers. That’s because
the low-power central processors do not handle video well. Therefore, manufacturers are
including low-power GPUs for video. Some Intel netbooks have Intel graphics, which
can’t (yet) be programmed for password cracking. Some contain nVidia’s ION graphics,
which is hardly faster at cracking passwords than the Atom CPU. The best choice these
days are the new AMD netbooks with the C-30, C-50, and E-350 processors that are a
combination of x86 CPU with a Radeon GPU on the same lower-power chip. A $280
Asus EEE PC 1015B or an $430 HP dm1z are the best netbooks for pen-testers at the
moment.

What about FirePro, Quadro, and Tesla?
Both AMD and nVideo make more expensive cards for high-end customers. These are actually the identical chips in the gaming cards, but sold for 10 times the price. They would be a foolish choice for password cracking.

There is a reason for the higher price. The companies put features into the chips for high-end customers, then disable those features for gamers. Thus, if you are a graphics artist using software to draw the next 3D movie, the version with the high-end features enabled are probably worth the price. But these features mean nothing to password cracking. Indeed, the high-end chips are slightly worse at password cracking: because high-end customers care about reliability, they run the chips at speeds slight slower (and cooler) than for gamers.

The more expensive version of the Radeon card is called "FirePro". The more expensive version of the GeForce card is called "Quadro".

But, there is a third high-end version of the GeForce card called "Tesla". This is just like the "Quadro" card (all high-end features) enabled -- but it's missing a the output port. You can't connect a monitor to it. It's purpose is just for GPU processing, like geological simulations to help find oil, or financial models to figure out the best stock price.
Password Cracking, Mining, and GPUs

Because they are missing the "display" portion, they use slightly less electrical power. People building supercomputers out of GPUs tend to choose the Tesla cards. If you rent "cloud computing" time using GPUs, they will probably be Tesla cards. I find this all a bit foolish -- GeForce or Radeon cards would be far more cost effective.

GPUs vs. FPGA vs. ASIC

Rather than doing password cracking in software, it should be possible to do it faster, cheaper, and with less electrical power using hardware like FPGAs or ASICs.

While this works in theory, it doesn’t work so well in practice. CPUs and GPUs are so cheap because their manufacturers sell them in enormous quantity. You could design your own chip that is 100 times faster than a cheap GPU, but it would cost you 200 times as much, per chip.

Some people do great things with hardware, such as Pico Computing, but most of the time, it’s just easier writing software for a mainstream chip, then let Moore’s Law make the chips go faster every year.

Building the ideal password cracking rig
Let’s say that you want to build the fastest computer (for cracking) for the cheapest price. Such a system will be driven by the cost of the graphics cards.

A relatively cheap, and simple, solution would be to buy three or four Radeon HD 6990 (as of June 2011) cards and stick them into a homebuilt computer. You’ll need a bigger power supply, a motherboard that supports four PCIe slots (spaced correctly for cards that are two-slots wide), and a slightly bigger case, but all of these are relatively common. Other than that, you only need a standard CPU, memory, and boot drive -- the cheaper the better (the less you spend on these, the more you can spend on more graphics cards).

This solution is probably best for pen-testers. Our time costs money. It doesn’t take long to assemble.
But for hobbists who enjoy messing around with hardware, the economics are a bit different. They might want to get fancy, for example, building a custom case using PCIe extender cables or even a PCIe splitter to fit 32 cards in a system. You only need PCIe 1x speed for password cracking, not the full PCIe 16x speed that’s used for gaming.

Regardless of the system you build, you probably need to worry about cooling. Such systems are going to produce a lot of heat. Moreover, you need to worry about where your cool air comes from, and where the hot air is going. It’s going to be an annoyance whether you are in a data center, in a lab, or installing it at home.

All this cooling will cause a lot noise (unless you are in a data center). Hobbists buy expensive components that cut down on the noise, like water cooling systems. I stick my computer in a closet that happens to have an air conditioning duct. In labs or at home, you may find yourself playing with ducts to get the cooling right and the noise reduced.

Windows, using commercial software like that from Elcomsoft, takes the least effort to setup and run, but Linux using free software gives you more control over what’s going
Password Cracking, Mining, and GPUs

on. For example, some people (such as Bitcoin miners) have reported that Windows can’t recognize more than 4 cards, whereas Linux has no problem. There is also the issue of systems only being able to use cards connected to monitors -- which requires either a monitor be plugged into each card, or a "dummy plug" be used to make the card think there is a monitor installed.

But, the thing to keep in mind is decreasing marginal returns. Buying a $250 Radeon card will increase cracking speeds by 20 times. Buying a second $250 Radeon card will only double the previous card’s speed. A single desktop with four Radeon HD 6990s for $3000 will increase cracking speed by 160 times. Buy a second such system, for another $3000, will only double your cracking speed after that.

Overclocking

Hobbiests spend a lot of time trying to overclock their systems. If they work hard enough
at it, they can get an extra 20% performance increase.

The trick for password cracking is to increase the speed of the GPU, but at the same time, decrease the speed of memory. Unlike graphics, GPU cracking doesn't use the memory. By lowering the memory speed, you lower power consumption, and lower the amount of heat generated. That power/heat can then be used to increase the speed of the GPU calculations.

Radeons come with an overclocking application on Windows, but it doesn’t allow you to change much. This utility will only let you overclock by 10%, but won’t let you underclock the memory.

A graphics card vendor named MSI has its own Radeon overclocking utility "Afterburner" that you can use for all Radeon cards, not just those sold by MSI: http://event.msi.com/vga/afterburner/download.htm. This will allow you do overclock the chip more, as well as underclock the memory.

If you are overclocking the card, it may cause your system to crash. If that happens, you may need to increase the voltage sent to the card.

If overclocking, and if you have increased voltage, your card will produce a lot more heat. You’ll probably have to adjust the fan speed to compensate, to lower temperatures back down to reasonable levels. You probably do not want to run your card above 80 degrees Celsius. On the other hand, fans aren’t designed to run at high speed for extended periods -- the more you jack up fan speed, the more likely it is for the fan to fail. If your card is running below 68 degrees Celsius, you might want to consider lowering the fan speed.

Overclocking, higher voltage, and higher temperatures will decrease the lifetime of the graphic chip before it fails. You probably don’t care: two years from now, when your overclocking madness causes the chip to fail, you’ll be upgrading to the latest GPU anyway.

**The economics of cracking**
Password Cracking, Mining, and GPUs

Putting a single $250 Radeon card in your desktop for password cracking makes sense. Building multiple cracking rigs for massive number crunching probably doesn't. The reason is that password cracking is an exponential effort.

Consider passwords chosen from an alphabet of UPPER and lower case, numbers, and $ymbols. That’s roughly 100 different characters. That means every letter we add to a password increases the difficulty of cracking by 100 times.

Let’s say you can crack all 8 character passwords within a day. It would then take you 100 days to crack a 9 character password and 27 years to crack a 10 character password. We can graph this effort on the following picture:

As you can see, it's a bit nonsensical. Below 9 characters, it's nearly zero effort to crack passwords. Above 9 characters, the line shoots almost straight upwards. Only around 9 characters do we see a line that isn't nearly-zero or nearly-infinite.
Password Cracking, Mining, and GPUs

That means there are three classes of passwords: those we can crack easily with a desktop computer (8 characters or fewer), those we cannot crack at all (10 characters or more), and those we can crack more of if we purchase more expensive computers (9 character passwords).

There is decreasing marginal returns to buying GPUs. Buying a single card increases cracking speed by 20 times. Buying a second GPU will only additionally increase speed by 2 times.

Buying a $3000 rig can increase cracking speed by 160 times. Buying a second $3000 rig will only increase cracking speed by an additional 2 times. All people have to do is add another character to the length of their password, increasing it’s complexity by 100 times, and defeating your investment.

On the other hand, there is the fact that your competitors have the same idea in mind. Let’s say that you go in and pen-test a company that hired a different pentesting firm last year. That other firm found passwords and cracked all the weak ones. You find the same password list. If you crack fewer passwords, you look like a poorer pentester than the previous firm. If you can crack a few more, you look like a better pentester.

The same is true of hackers. You can assume the target company has already fixed all it’s weak passwords -- but where "weakness" is defined as "crackable by one GPU". If you come in with two GPUs, you’ll find a few more passwords.

This is of particular interest to Bitcoin miners, where it’s essentially a race against other miners to find the latest hash. Whereas twice the computing power does not equal twice the number of passwords cracked, twice the power does mean twice the earning power for Bitcoins.

**Bitcoin mining benchmarks**

Password cracking and Bitcoin mining are essentially the same thing. You can therefore leverage their work in figuring out what hardware you want for cracking.
A good reference is the list of hardware at https://en.bitcoin.it/wiki/Mining_hardware_comparison.

I've selected a few of the numbers from the link above, as well as benchmarked my own computers.

<table>
<thead>
<tr>
<th>MH/s</th>
<th>Hardware</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.2</td>
<td>ARM Cortex-A8</td>
<td>CPU in my iPhone</td>
</tr>
<tr>
<td>0.6</td>
<td>ARM Cortex-A9 dual</td>
<td>CPU in my iPad</td>
</tr>
<tr>
<td>1.1</td>
<td>Intel Atom N270</td>
<td>My pen-testing netbook CPU</td>
</tr>
<tr>
<td>1.8</td>
<td>nVidia ION</td>
<td>A common netbook GPU for Atom CPUs</td>
</tr>
<tr>
<td>2.5</td>
<td>Core 2 Duo 2.13 GHz</td>
<td>My MacBook Air CPU</td>
</tr>
<tr>
<td>6.1</td>
<td>nVidia GT 320M</td>
<td>My MacBook Air GPU</td>
</tr>
<tr>
<td>6.2</td>
<td>AMD C-30</td>
<td>Asus $280 netbook with GPU/CPU combo</td>
</tr>
<tr>
<td>11.0</td>
<td>AMD E-350</td>
<td>HP dm1z $450 netbook with GPU/CPU combo</td>
</tr>
<tr>
<td>17.0</td>
<td>Radeon HD 6490M</td>
<td>2011 MacBook Pro</td>
</tr>
<tr>
<td>19.2</td>
<td>Core i7 980x</td>
<td>My desktop, 6-core 3.3 GHz, hyperthreaded, top-of-the-line CPU</td>
</tr>
<tr>
<td>21.0</td>
<td>PS3</td>
<td>Playstation 3 using the Cell GPU</td>
</tr>
<tr>
<td>100.0</td>
<td>Tesla M2050</td>
<td>Amazon EC2 cloud computer w/ Tesla card</td>
</tr>
<tr>
<td>300.0</td>
<td>Radeon HD 5830</td>
<td>$109 card popular with miners -- if you can find one</td>
</tr>
<tr>
<td>314.0</td>
<td>Radeon HD 6950</td>
<td>$240 @Newegg and probably what you should buy</td>
</tr>
<tr>
<td>358.0</td>
<td>Radeon HD 6970</td>
<td>My desktop's graphics card, cost $330</td>
</tr>
</tbody>
</table>
Password Cracking, Mining, and GPUs

### SSE

SSE is the name for GPU-like instructions that are part of the CPU. They operate on 4 numbers at a time, and therefore, are 4 times faster than normal instructions for repetitive tasks.

Modern processors, like the Intel Atom, Core2, and Core i3/i5/i7, as well as AMD Athlon/Phenom/etc. processors, all can execute two SSE integer instructions per clock cycle. That means pretty much that you just need to look at MHz in order to figure out which processor will crack passwords faster.

This also applies to Intel’s energy efficient Atom processor. While the Atom is notorious for being slower on most tasks, it’s just as fast, per-core and per-MHz, as the other processors. Thus, a 1.6 GHz Atom will perform the same as a 1.6 GHz Core2 or 1.6 GHz
Password Cracking, Mining, and GPUs

AMD processor at password cracking -- but at about half the power. In addition, the GeForce-based ION graphics chip designed to go with the Atom hardly accelerates password cracking.

MacBook Air

Whereas I use netbooks for pen-testing, I use a MacBook Air for everything else (programming, writing blogposts). I’m not a fan of Apple’s operating system, I usually run Windows or Linux on it.

My MacBook is faster at password cracking than the older netbooks, but is quite a bit behind the latest Radeon-based netbooks. My next pen-testing netbook is likely going to be the HP dm1z.

HP dm1z

At $429, this is expensive for a "netbook", but it has 4 features that make it stand out.

1. It has the GPU/CPU combo from AMD. Not only is its CPU faster (dual core), but its GPU is a lot faster.
Password Cracking, Mining, and GPUs

2. It comes with 3-gigs of RAM, expandable to 8-gigs. Most "netbooks" come with 1-gig, expandable to 2-gigs.
3. It comes with Gigabit Ethernet, whereas other "netbooks" come with only 100-mbps Ethernet.
4. HP claims 9.5 hour battery life, which is at the top end of the range for "netbooks".

Thus, while I’m tempted by its cheaper cousin the $279 Asus, I’ve ordered the dm1z to take to DefCon. I’ll be blogging successes/failures with it in a few days.

MacBook Pro

The 15-inch MacBook Pro is probably going to be the notebook of choice for a lot of hackers, and probably has the best password cracking speed of anything short of a specialized gaming notebook.

Currently, there are some quirks with Mac OS X bitcoin mining software, compared to Windows or Linux. It should be getting as much as twice the benchmarks posted above.

Radeon HD 6950

If you do password cracking, you should get one, maybe two, of these cards and stick them in your existing desktop computer. They give the greatest bang-for-the-buck right now. An older Radeon HD 5830 are probably better bang-for-the-buck at half the price, but all the Bitcoin miners have snapped them up, so you can’t find any.
The 6950 is slight slower than the 6970, but at 66% of the price. The fastest single card, the 6990, combines two 6950 GPU chips on a single card but at three times the price.

Six months from now (Juned 2011) the situation will have changed, but in all probability, a $250 will still provide the best bang for the buck.

**Tesla**

As the benchmarks show, the Tesla card is 10 times the price, but 1/3 the performance, of a Radeon HD 6950 card. That's 30x price-performance difference.

The economics don’t get any better using a Tesla in Amazon’s EC2 instances. You can currently make money mining bitcoins using Radeon cards, but you’d lose a lot of money trying to mine bitcoins on Amazon.

**What you crack**

I thought I’d list the common things that hackers find themselves needing to crack. It’s not really relevant to GPUs, but I thought I’d mention it for completeness.

**Bitcoin mining**

A fixed number of new bitcoins are generated per day, and it’s a race to find the
Password Cracking, Mining, and GPUs

matching hash before anybody else does. The winner gets the bitcoins. It uses SHA256, which is exactly like SHA256 passwords.

There is a lot of free bitmining software on the Bitcoin forums.

WPA passwords

Home users, and many businesses, use WPA, which is protected by only a simple password. In order to make it more difficult, the WPA standard requires a minimum of 8 characters, and rather than protect it by hashing the password once, it re-hashes it 4000 times -- making the computational difficulty to be around a 10-character password.

Ten letters in a password is probably beyond the ability for "brute-force" cracking, which tries all combinations, unless you make certain assumptions, such as assuming the person used only lower-case and numbers (which is a valid assumption for most passwords). Most cracking is therefore done using a dictionary of known passwords, followed by "mutations" (such as adding a 4-digit number onto the end).

Because the password is "salted" with the SSID, you can’t use rainbow tables to get the hash.

There is lot of good software for doing this. I’ve used the free software "pyrit" and the commercial package from "Elcomsoft" in the past. The graph above of relative WPA
cracking speeds is for the Elcomsoft package using last year's cards.

**NTLM challenge-response**

Windows passwords aren't "salted", which means it’s easier to Rainbow crack them than to crack them.

However, you often see "challenge-response" exchanges on the wire. This requires cracking in order to break. You see these with Windows-specific protocols like SMB and MS-RPC. In addition, you'll see these as an optional authentication on other protocols, such as LEAP authentication for WiFi, or NTLMv2 inside e-mail and HTTP headers.

**Salted passwords on a hacked server**

When a hackers (or pen-tester) breaks into a server, they will grab the password file or database.

Stupid sysadmins either have the passwords in cleartext (no cracking needed) or in simple MD5 hashes (cracked with Rainbow tables). Smart sysadmins "salt" the passwords, which requires cracking.

**Documents**

PDF, ZIP, RAR, and Word/Excel files are often encrypted. Such files might contain secrets useful for a hacker. Reportedly, Wikileaks had to decrypt an encrypted ZIP file containing the famous "Collateral Murder" video from Iraq.

Cracking password-protected documents is the most common feature of commercial software, since home users and businesses need it when they forget their password. There are lots of companies that sell GPU accelerated software for this, such as Elcomsoft.

**Conclusion**
Buying a $250 GPU that increases password cracking speed 20 times is a no-brainer. Buying a notebook computer based on GPU is probably a wise idea for pen-testers.

But passwords are a little strange. They grow exponentially in complexity, which means you get decreasing marginal returns from buying more hardware. Thus, while buy a graphics card (or maybe two) is cost effective, massive investments in hardware are unlikely to crack that many additional passwords.

Of course, if you are Bitcoin mining, then the more GPUs the better. Even after recent wild fluxuations in bitcoin prices, it’s still profitable at the moment.
OFFLOADING your software and data to a cloud computing service has never been easier.

Apple last week became the latest tech company - after Google and Amazon - to offer cheap online storage, with its new iCloud service allowing users to access music, documents and other files from any Apple device. But cloud services could also be used to launch attacks, send spam and commit fraud.

"Right now it's just a few attacks, most aren't well publicised and a lot can go undetected," says Kassidy Clark of the Delft University of Technology in the Netherlands. "As long as cloud service providers are not taking proactive steps to prevent these things, I think this trend will increase."

As well as basic online storage, firms such as Amazon, which provides the largest cloud service, also offer virtual computing. This allows people to rent as many "virtual computers" as they need.

Now Clark and colleagues have investigated how the cloud could be used to build a botnet, a network of infected computers under an attacker's control. Traditional botnets are built over time by taking control of ordinary people's computers without their knowledge, but a cloud botnet - or botcloud - can be put together in a couple of minutes just by purchasing space in the cloud with stolen credit card details. "It makes deployment much faster," says Clark, who presented his findings at the CLOSER cloud computing conference in Noordwijkerhout, the Netherlands, last month. "You don't have to wait months for millions of machines around the world to get infected."
Botclouds: A Cyber Attacker's Dream

To find out just how easy it is to construct a botcloud, Clark and colleagues hired 20 virtual computers from a leading cloud service provider for around €100 and used them to carry out attacks on their own web server. They first attempted a distributed denial of service (DDoS) attack, which floods a target with massive amounts of traffic. The botcloud pumped out 20,000 page requests per second and brought the server down in just 10 seconds.

Clark also built a larger botcloud and used it to simulate "click fraud" - clicking links in pay-per-click adverts in order to generate fraudulent revenue. Advertising companies normally stop this by tracking the internet protocol (IP) address of each individual computer and blocking one if it clicks a link too many times. The researchers circumvented this defence by setting up a botcloud of 1000 virtual computers, each with its own address. Neither botcloud attack was detected or shut down by the cloud provider.

So are botclouds being used? There were certainly rumours that the recent attack on Sony's PlayStation Network was carried out via Amazon servers rented using stolen credit cards, but these have not been substantiated. "We have seen spam coming from some of these environments, but not on a massive scale," says Paul Wood, a senior analyst at Symantec.cloud, which provides cloud-based security services. He says that it is even possible for a virtual computer in the cloud to become infected by an ordinary botnet, because cloud users don't normally run anti-virus software.

Thomas Roth, a security researcher in Cologne, Germany, who recently showed how to use Amazon's servers to crack Wi-Fi passwords, agrees the lack of anti-virus protection in the cloud is a problem. "I think that Amazon should provide infrastructure for doing vulnerability assessments and virus scans," he says.
"Amazon Web Services employs a number of mitigation techniques, both manual and automated, to prevent the misuse of the services," Amazon told New Scientist. "We have automatic systems in place that detect and block many attacks before they leave our infrastructure."

But Wood warns that attacks from the cloud could easily take off in countries with more lax web policing. "It's only a matter of time before a Russian or Chinese equivalent of Amazon offers similar services," agrees Clark. "You put malicious or illegal software there, it doesn't matter, they will never take you offline."
The National Security Agency is working with Internet service providers to deploy a new generation of tools to scan e-mail and other digital traffic with the goal of thwarting cyberattacks against defense firms by foreign adversaries, senior defense and industry officials say.

The novel program, which began last month on a voluntary, trial basis, relies on sophisticated NSA data sets to identify malicious programs slipped into the vast stream of Internet data flowing to the nation’s largest defense firms. Such attacks, including one last month against Bethesda-based Lockheed Martin, are nearly constant as rival nations and terrorist groups seek access to U.S. military secrets.

“We hope the . . . cyber pilot can be the beginning of something bigger,” Deputy Defense Secretary William J. Lynn III said at a global security conference in Paris on Thursday. “It could serve as a model that can be transported to other critical infrastructure sectors, under the leadership of the Department of Homeland Security.”

The prospect of a role for the NSA, the nation’s largest spy agency and a part of the Defense Department, in helping Internet service providers filter domestic Web traffic already had sparked concerns among privacy activists. Lynn’s suggestion that the program might be extended beyond the work of defense contractors threatened to raise the stakes.

James X. Dempsey, vice president for public policy at the Center for Democracy & Technology, a civil liberties group, said that limiting the NSA’s role to sharing data is “an elegant solution” to the long-standing problem of how to use the agency’s expertise while avoiding domestic surveillance by the government. But, he said, any extension of the program must guarantee protections against government access to private Internet traffic.

“We wouldn’t want this to become a backdoor form of surveillance,” Dempsey said.

Officials say the pilot program does not involve direct monitoring of the contractors’ networks by the government. The program uses NSA-developed “signatures,” or fingerprints of malicious code, and sequences of suspicious network behavior to filter the Internet traffic flowing to major defense contractors. That allows the Internet providers to disable the threats before an attack can penetrate a contractor’s servers. The trial is testing two particular sets of signatures and behavior patterns that the NSA has detected as threats.

The Internet carriers are AT&T, Verizon and CenturyLink. Together they are seeking to filter the traffic of 15 defense contractors, including Lockheed, Falls Church-based CSC, McLean-based
NSA Allies With Internet Carriers to Thwart Cyber Attacks Against Defense Firms

SAIC and Northrop Grumman, which is moving its headquarters to Falls Church. The contractors have the option, but not the obligation, to report the success rate to the NSA’s Threat Operations Center.

All three of the Internet carriers declined to comment on the pilot program. Several of the defense contractors declined to comment as well.

Partnering with the major Internet providers “is probably the technically quickest way to go and the best way to go” to defend dot-com networks, said Gen. Keith B. Alexander, who heads the NSA and the affiliated U.S. Cyber Command at Fort Meade, testifying before Congress in March.

The premise of this strategy is that combining the providers’ ability to filter massive volumes of traffic — a large Internet carrier can monitor up to 100 gigabits per second — with the NSA’s expertise will provide a greater level of protection without violating privacy laws.

But the initiative stalled for months because of numerous concerns, including Justice Department worries that the program would run afoul of privacy laws forbidding government surveillance of private Internet traffic. Officials have, at least for now, allayed that concern by saying that the government will not directly filter the traffic or receive the malicious code captured by the Internet providers. The Department of Homeland Security is a partner in the pilot program.

“The U.S. government will not be monitoring, intercepting or storing any private-sector communications,” Lynn said. “Rather, threat intelligence provided by the government is helping the companies themselves, or the Internet service providers working on their behalf, to identify and stop malicious activity within their networks.”

But civil liberties advocates are worried that a provision in the White House’s recent legislative proposal on cybersecurity could open the way to government surveillance through public-private partnerships such as this one. They are concerned that the proposal would authorize companies to share vast amounts of communications data with the federal government.

“The government needs to make up its mind about whether it wants to protect networks or collect intelligence,” Dempsey said.

Although this NSA technology is more sophisticated than traditional anti-virus programs, it still can screen only for known threats. Developing detection and mitigation strategies for emerging new threats is more difficult.

The program also does not protect against insider threats or employees who deliberately leak material. Nor will it protect a network from penetration by hackers who have compromised security software, enabling them to log in as if they were legitimate users. That is what happened recently when security firm RSA’s SecurID tokens were compromised, enabling hackers to penetrate
NSA Allies With Internet Carriers to Thwart Cyber Attacks Against Defense Firms

Lockheed Martin’s computers. Lockheed said no customer, program or employee personal data were compromised.

The pilot program has been at least a year in the making. Providers and companies were concerned that they would be vulnerable to lawsuits or other sanctions if they allowed the government to filter the traffic or shared network data with the government. The NSA, meanwhile, was concerned about the classified data getting into the hands of adversaries.

The Internet carriers that are part of the pilot are not being paid to prepare their systems for it, an effort that industry officials said costs millions of dollars. The providers will work with the companies they currently serve. In some cases, they already provide a similar service of filtering for malicious traffic using their own threat data.

Lynn’s speech also appeared to outline key elements of the Pentagon’s cybersecurity strategy, an unclassified version of which is due out soon. The strategy, said experts and analysts who have been briefed on it, focuses on building defenses and a framework for deterrence. It also makes clear the military’s prerogative to use cyberwarfare and other traditional military means if the United States is attacked or becomes engaged in hostilities with an adversary.

“First we must raise the level of protection in government and military networks,” Lynn said Thursday. “We must ready our defense institution to confront cyberthreats, because it is clear any future conflict will have a cyber dimension.”
Is cyber crisis the new normal?  
By Philip Ewing Friday, June 17th, 2011 10:58 am

Once you get through this story by a Reuters all-star team of Phil Stewart, Diane Bartz, Jim Wolf and Jeff Mason, you’ll probably be depressed. America’s public and private institutions, they write, are effectively in a state of cyber-siege, or, if you prefer, cyber-chaos, enduring attacks from spies who want to vacuum up secrets, enemies who want to bring sites down, or vandals who just want to deface as much as they can. As you’ve read here before, there’s no telling how much classified information has already been lost to hacking, nor is there any guarantee DoD’s new cyber-strategy will afford any immediate help, beyond its hazy threat of real-world retaliation for cyber attacks.

The government is trying to help, the Reuters team writes, but things are not going well: “Notwithstanding the military’s efforts, however, the overall gap appears to be widening, as adversaries and criminals move faster than government and corporations, and technologies such as mobile applications for smart phones proliferate more rapidly than policymakers can respond, officials and analysts said.” The anarchic nature of the web, and the nature of the American institutions that rely on it — slow-moving, disconnected at best and dysfunctional at worst — means you can’t just send Delta to go kill a guy and make this threat go away.

Lawmakers and public officials often talk about a hypothetical future in which the U.S. comes under a major cyber attack — incoming Secretary Panetta warned the Senate Armed Services Committee that a cyber attack could be the “next Pearl Harbor.” But the state of American cyber-security today already seems to be in crisis, with constant headlines about the latest cyber-damage somewhere. (Even GanGovMedCorp’s Military Times newspapers were attacked!) Is this just how it’s going to be from here on out, so long as criminal and state-sponsored black hatters can always keep a step ahead of the government and industry?

If you want to get a taste of just how dire our situation is, take a look at the Reuters team’s breakdown of how far the U.S. remains from any coherent plan for a solution to the cyber-problem:

Experts say that one of the toughest challenges of cyber defense is, oddly, definitions. What constitutes “cyber”? Computers and digital networks, certainly. But how about digitized pictures or video streams from a pilotless Predator drone flying over Pakistan?

Who is responsible for protecting what? Where does national security begin and privacy end?

“The other big problem is lack of policy,” said one former U.S. official. “(We) lack policy
because we lack consensus. We lack consensus because we haven’t had an informed debate. We lack an informed debate because we don’t have a common pool of data. And we don’t have a common pool of data because we don’t share it.”

Washington will never just throw up its hands and say, ‘well, this is too hard. We give up.’ But amid the endless calls for “debate” — “oh, we can’t do anything until we’ve had a good debate!” — there should probably also be some calls for realism: Until or unless the authorities get this figured out, Americans should evidently expect cyber-snooping, hacking and online vandalism all to become facts of life.
Old worm won't die after 2008 attack on military

By Phil Stewart and Jim Wolf
WASHINGTON | Thu Jun 16, 2011 11:23pm EDT

(Reuters) - Three years after what the Pentagon called the most significant breach of U.S. military networks ever, new versions of the malware blamed for the attack are still roiling U.S. networks, Reuters has learned.

The malware at issue, known as "agent.btz," in 2008 infiltrated the computer systems of U.S. Central Command, which was running the wars in Iraq and Afghanistan.

The attack established what Deputy Defense Secretary William Lynn called "a digital beachhead" for a foreign intelligence agency to attempt to steal data.

The Pentagon last year disclosed its operation to counter that attack, known as Buckshot Yankee. But new, more potent variations of agent.btz are still appearing.

"We can definitely say that it's not limited to government computers, it never has been, and that it hasn't gone away," said an official of the Department of Homeland Security, which leads U.S. efforts to secure federal nonmilitary computer networks, often described as the Internet's "dot.gov" domain.

"It's very persistent and it keeps evolving," the official said. "You're constantly seeing new, better versions of it. So it's a challenge to keep ahead of it."

"It's quite prolific," the official added, speaking on condition of anonymity because of the matter's sensitivity. The official did not specify precisely which networks have been affected or the extent of the damage.
FOREIGN SPY AGENCY

U.S. officials have said a foreign spy agency was responsible for the 2008 attack, which occurred when an infected flash drive was inserted into a U.S. military laptop at a base in the Middle East.

But they have never publicly named which one. Reuters has learned that experts inside and outside of the U.S. government strongly suspect that the original attack was crafted by Russian intelligence.

Information about the origin of the suspected attackers, however, is still closely held and Pentagon officials refuse to discuss it. People familiar with the matter spoke to Reuters on condition of anonymity and did not explain why Russia was the top suspect.

Buckshot Yankee led to Defense Secretary Robert Gates' order in June 2009 to create the military's new Cyber Command, which became operational last year.

"That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control," Lynn wrote in the journal Foreign Affairs last fall.

"It was a network administrator's worst fear: a rogue program operating silently, poised to deliver operational plans into the hands of an unknown adversary," he said.

EVADES ANTI-VIRUS DEFENSES

Anup Ghosh, a former senior computer scientist at the Pentagon's Defense Advanced Research Projects Agency (Darpa), said agent.btz was configured in a way that made it likely to remain a threat.
Old Worm Won't Die After 2008 Attack on Military

It reaches out to download new code, enabling it to change its "signature" continuously and evade anti-virus software running on host networks, said Ghosh, who worked on securing military systems while at Darpa from 2002 to 2006 and now heads Invincea, a cybersecurity software company.

"Old worms never die," he said. "They simply re-morph and rear their head again."

Michael McConnell, the Director of National Intelligence from 2007 to 2009, indicated on Thursday night that he considered Russia's cyber espionage capabilities as outpacing China's.

China is "literally taking terabytes of data," McConnell said during a panel discussion in New York about cyber threats moderated by Reuters Editor-in-Chief Stephen Adler.

But "there are other nation-states that are better, so when they take things they're not observed as frequently," McConnell said. Pressed on whether he was referring to Russia, McConnell nodded yes.

McConnell, in an interview after the session, said he knew who was behind the 2008 attack on Central Command but it was a classified matter that he would not discuss publicly. "What's been said can be said," McConnell said.

Could the code have been written in a third country in an effort to mask the attack mastermind's digital fingerprints?

So thinks Jeffrey Carr, author of the book Inside Cyber Warfare: Mapping the Cyber Underworld and a consultant to the U.S. and allied governments on Russian and Chinese cyber strategy and tactics as well as emerging threats.

"The agent.btz sample that I've seen has indicators that it was created in China, which doesn't exclude Russia," he said by email. "In fact, if I were a Russian hacker running that 2008 operation against USCENTCOM, I'd purposefully use malware that was
developed in China, Korea or elsewhere."

"I wouldn't want anything to point back to me or whoever hired me," Carr said.

(Editing by Warren Strobel and David Storey)
Kissinger, Huntsman: U.S., China need cyber detente

By Paul Eckert and Daniel Magnowski
NEW YORK/SINGAPORE | Tue Jun 14, 2011 7:30pm EDT

(Reuters) - The United States and China need to reach an agreement to restrict cyber attacks and designate some areas as off limits to hacking, two former senior U.S. officials said on Tuesday.

Henry Kissinger, an architect of the opening of U.S. relations with China in the 1970s, told a Thomson Reuters event that Washington and Beijing both had significant espionage capabilities and the key was finding a way to discuss them.

Jon Huntsman, the former U.S. ambassador to China, likened raising cyber attacks with Beijing to the challenge of discussing missile defense and the military use of space -- issues that are also highly sensitive to the Chinese.

"At some point, we are going to have to develop a context in which we can actually discuss this and, I would think, draw some red lines around areas that we don't want them into and they might not want us into," said Huntsman, who left China in April to plan his presidential election campaign, and was speaking at the same event.

Their calls for a cyber detente follow a blitz of hacking attacks on major U.S.-based institutions in recent weeks, including the International Monetary Fund, the Senate, and companies such as Citigroup and Lockheed Martin.

Chinese entities have been suspected in attacks on Google e-mail accounts of U.S. officials and Chinese activists, though Beijing has denied involvement and said it too is a victim of international hacking.
"China has also many times reiterated that we are willing to open up exchanges and cooperation with the international community about Internet security," Foreign Ministry spokesman Hong Lei said earlier on Tuesday.

Kissinger, former secretary of state, said that without an overall agreement, relations over the issue would likely deteriorate. "If you take it case by case it will lead to accusations and counter-accusations," he said.

The spate of security breaches prompted NATO to endorse a cyber defense policy on Monday after a meeting last week. NATO officials say the policy focuses on protecting the alliance's computer networks and defense planning processes, and allows for broader consultations on cyber threats.

"If there's a cyber threat, NATO has consultation mechanisms and may consult about anything. But the ambition now is to defend NATO bodies, NATO agencies, NATO structures. This is what we are working concretely on," said a NATO official.

CALLS FOR INTERNATIONAL ACTION

Security experts say the borderless nature of the Web requires a coordinated global response against hacking. The view that cyber security is a technical problem, rather than a strategic one, has meant that it has not been a priority.

India's top IT bureaucrat, R. Chandrasekhar, said high-level cooperation between states was needed. India's computer networks have frequently been attacked, with the hackers suspected to be from China and Pakistan.

"Government to government contacts are there...(but) at the middle level," he said. "Concerted efforts are needed. We are yet to see the emergence of a clear organizational
US, China Need Cyber Detente

Neelie Kroes, European Commission Vice President for the Digital Agenda, said there are plans for a pan-EU network to coordinate responses to cyber attacks by 2012, and the EU has a strategic partnership with the U.S. on cybercrimes.

"Governments worldwide need to address cybersecurity threats, and drafting strategies is an important step toward doing so," Kroes said.

Peter Coroneos, co-founder of the International Internet Industry Association and head of Australia's industry body, called on world leaders to put cyber security on the agenda at forums such as the G20 and urge "slower-moving" nations to take a stand against hacking.

KOREA DRAFTS PLAN, INDONESIA WARNS OF RISKS

South Korea said on Tuesday it was drawing up a cyber security master plan, but some other Asian governments appeared to have no blueprint for tackling the threat.

Indonesia, a rapidly growing G20 country, warned that hackers could cause serious damage to its institutions.

"Every day, not every month, but every day, we get 1.2 million hacker attacks in Indonesia, both from within the country and outside," said Gatot Dewa Broto, Indonesia's communication and information ministry spokesman.

"If we don't improve (our capabilities) we could face a possible public and commercial institutional collapse."

But getting nations to work together to combat cyber security won't be easy, experts said, pointing to differing ideologies and goals.

The Chinese government, for example, may be more interested in tracking down
dissidents on the Internet than in prosecuting criminal hackers.

"At the end of the day, in my view, a lot of the Chinese solution for hackers is more aggressively finding out who's doing what in cyberspace," said Stewart Baker, a former Department of Homeland Security official now at the law firm Steptoe and Johnson LLP.

"These are the kinds of things that are likely to make the world a little less safe for hackers but also for the color revolutions," he said. "If you help law enforcement around the world you're helping the British bobbies. but you're also helping Russian, Iranian and Chinese security forces who are less attractive in the range of things that they do," he said.

Others said they saw room for progress between the U.S. and China on questions such as the use of the Internet for child porn and terrorism.

"Law enforcement -- that would be a good place to start," said Jim Lewis, a cyber expert at the Center for Strategic and International Studies. "Everyone can agree that child porn is bad and you don't want to support terrorism."

Lewis also said that Beijing had many reasons to crack down on cybercrime. "Nobody likes cybercrime, including the Chinese. They don't like cybercrime. They worry about their hackers turning on the government."

(Additional reporting by Jeff Mason, David Brunnstrom, Christopher Lecoq; Writing by Tiffany Wu; Editing by Martin Howell)
If we discovered Chinese explosives laid throughout our national electrical system, we'd consider it an act of war. China's digital bombs pose as grave a threat.

By RICHARD CLARKE

In justifying U.S. involvement in Libya, the Obama administration cited the "responsibility to protect" citizens of other countries when their governments engage in widespread violence against them. But in the realm of cyberspace, the administration is ignoring its primary responsibility to protect its own citizens when they are targeted for harm by a foreign government.

Senior U.S. officials know well that the government of China is systematically attacking the computer networks of the U.S. government and American corporations. Beijing is successfully stealing research and development, software source code, manufacturing know-how and government plans. In a global competition among knowledge-based economies, Chinese cyberoperations are eroding America's advantage.

The Chinese government indignantly denies these charges, claiming that the attackers are nongovernmental Chinese hackers, or other governments pretending to be China, or that the attacks are fictions generated by anti-Chinese elements in the United States. Experts in the U.S. and allied governments find these denials hard to believe.

Three years ago, the head of the British Security Service wrote to hundreds of corporate chief executive officers in the U.K. to advise them that their companies had in all probability been hacked by the government of China. Neither the FBI nor the Department of Homeland Security has issued such a notice to U.S. executives, but most corporate leaders already know it.

View Full Image
Some, like Google, have the courage to admit that they have been the victims of Chinese hacking. We now know that the "Aurora" attack (so named by the U.S. government because the English word appears in the attack software) against Google in 2009 also hit dozens of other information technology companies—allegedly including Adobe, Juniper and Cisco—seeking their source code. Aurora wasn't an isolated event. This month Google renewed its charge against China, noting that the Gmail accounts of senior U.S. officials had been compromised from a server in China. The targeting of specific U.S. officials is not something that a mere hacker gang could do.

The Aurora attacks were followed by systematic penetrations of one industry after another. In the so-called Night Dragon series, attackers apparently in China went after major oil and gas companies, not only in the U.S. but throughout the world. The German government claims that the personal computer of Chancellor Angela Merkel was hacked by the Chinese government. Australia has also claimed that its prime minister was targeted by Chinese hackers.

Recently the computer-security company RSA (a division of EMC) was penetrated by an intrusion which appears to have stolen the secret sauce behind the company's SecureID. That system is widely used to protect critical computer networks. And this month, the largest U.S. defense contractor, Lockheed, was subject to cyberespionage, apparently by someone using the stolen RSA data. Cyber criminals don't hack defense contractors—they go after banks and credit cards. Despite Beijing's public denials, this attack and
many others have all the hallmarks of Chinese government operations.

In 2009, this newspaper reported that the control systems for the U.S. electric power grid had been hacked and secret openings created so that the attacker could get back in with ease. Far from denying the story, President Obama publicly stated that "cyber intruders have probed our electrical grid."

There is no money to steal on the electrical grid, nor is there any intelligence value that would justify cyber espionage: The only point to penetrating the grid's controls is to counter American military superiority by threatening to damage the underpinning of the U.S. economy. Chinese military strategists have written about how in this way a nation like China could gain an equal footing with the militarily superior United States.

What would we do if we discovered that Chinese explosives had been laid throughout our national electrical system? The public would demand a government response. If, however, the explosive is a digital bomb that could do even more damage, our response is apparently muted—especially from our government.

Congress hasn't passed a single piece of significant cybersecurity legislation. When the Chinese deny senior U.S. officials' claims (made in private) that Beijing is stealing terabytes of data in the U.S., Congress should not leave the American people in doubt. It should demand answers to basic questions:

What does the administration know about the role of the Chinese government in cyberattacks on public and private computer networks in the United States?

If there is widespread Chinese hacking of sensitive U.S. networks and critical infrastructure, what has the administration said about it to the Chinese government? Specifically, did President Obama raise concerns about these
attacks with Chinese President Hu Jintao at the White House this spring?

Since defensive measures such as antivirus software and firewalls appear unable to stop the Chinese penetrations, does the administration have any plan to address these cyberattacks?

In private, U.S. officials admit that the government has no strategy to stop the Chinese cyberassault. Rather than defending American companies, the Pentagon seems focused on "active defense," by which it means offense. That cyberoffense might be employed if China were ever to launch a massive cyberwar on the U.S. But in the daily guerrilla cyberwar with China, our government is engaged in defending only its own networks. It is failing in its responsibility to protect the rest of America from Chinese cyberattack.

Mr. Clarke was a national security official in the White House for three presidents. He is chairman of Good Harbor Consulting, a security risk management consultancy for governments and corporations.
The Chinese military wants to beef up its cyberdefense efforts as it anticipates greater threats originating from the U.S.

"The U.S. military is hastening to seize the commanding military heights on the Internet, and another Internet war is being pushed to a stormy peak," the Chinese military wrote in its official newspaper, Liberation Army Daily. "Their actions remind us that to protect the nation's Internet security, we must accelerate Internet defense development and accelerate steps to make a strong Internet army."

Though Liberation Army Daily isn't an official mouthpiece for the Chinese government, Reuters, which first reported on the story, points out that it typically reflects the official opinion of China's ruling party. The Chinese military's calls for a stronger "Internet army" comes as China finds itself under fire for alleged hacking attempts on U.S. corporations and government organizations.

Earlier this month, Google announced that the Gmail accounts of top U.S. government officials and Chinese political activists were targeted in a phishing attack designed to gain access to the users' accounts. Google stopped short of blaming the Chinese government, but the search giant said that the attacks seemed to originate from Jinan, China, home to a Chinese government intelligence division. That breach followed a hacking attempt in 2009 against Google and several other companies across the finance, technology, and chemical industries. Google said at the time that the "highly sophisticated and targeted attack," which also appeared to originate in China, led to the theft of the company's intellectual property.

In both cases, the Chinese government denied charges that it was behind the attacks.

Earlier this year, RSA was targeted in what it called an "extremely sophisticated
cyberattack" aimed at stealing data shielded by its SecurID platform, which is widely used by the U.S. government and major corporations. The stolen information was used last month in attacks on Lockheed Martin, Northrop Grumman, and other U.S. government contractors, forcing Lockheed to replace 45,000 SecurID tokens. Though the Chinese government was not specifically targeted in the attacks, former U.S. national security official Richard Clarke wrote in The Wall Street Journal yesterday that the U.S. knows where to place blame.

"Senior U.S. officials know well that the government of China is systematically attacking the computer networks of the U.S. government and American corporations," Clarke wrote in the op-ed piece for the Journal. "Beijing is successfully stealing research and development, software source code, manufacturing know-how and government plans."

Even worse, Clark said, the U.S. government "has no strategy to stop the Chinese cyberassault." But the U.S. doesn't seem to be alone. The Chinese military wrote that the country's "Internet security defenses are still very weak."

At this point, it seems that both sides are focusing on what Clarke calls "active defense," a term that he says the Pentagon uses to mean "offense," amid a "daily guerrilla cyberwar" between the two countries. There's no telling where the cyberwar between the U.S. and China is headed. But the Wall Street Journal reported last month that the U.S. is mulling a policy that would define cyberattacks as an act of war, paving the way for the government to respond with military might in the event that it's attacked via the Web.
New Leader for Navy's Cyber Forces as Pentagon Gets Cyberwar Guidelines

New Leader For Navy's Cyber Forces As Pentagon Gets Cyberwar Guidelines
(ASSOCIATED PRESS 22 JUN 11)

VIRGINIA BEACH – A new commander takes control of the Navy's Cyber Forces as the president lays out guidelines for military use of cyberattacks and other computer-based operations against enemies and for routine espionage.

Rear Adm. Gretchen S. Herbert relieved Rear Adm. Thomas P. Meek in a Wednesday morning ceremony at Joint Expeditionary Base Little Creek.

Cyber Forces Command handles cryptology/signals intelligence, cyber, electronic warfare, information operations, intelligence, networks, and space.

Meek took command in May 2010 and will now serve as Director of Military Support at the National Geospatial-Intelligence Agency in Springfield.

President Barack Obama's executive orders that detail when the military must seek presidential approval for a specific cyber assault on an enemy and weave cyber capabilities into U.S. war fighting strategy, defense officials and cyber security experts told The Associated Press.

Signed more than a month ago, the orders cap a two-year Pentagon effort to draft U.S. rules of the road for cyber warfare, and come as the U.S. begins to work with allies on global ground rules.

The guidelines are much like those that govern the use of other weapons of war, from nuclear bombs to missiles to secret surveillance, the officials said.

In a broad new strategy document, the Pentagon lays out some of the cyber capabilities the military may use during peacetime and conflict. They range from planting a computer virus to using cyberattacks to bring down an enemy's electrical grid or defense network.

"You don't have to bomb them anymore. That's the new world," said James Lewis, cybersecurity expert at the Center for Strategic and International Studies.

The new Pentagon strategy, he said, lays out cyber as a new warfare domain and stresses the need to fortify network defenses, protect critical infrastructure and work with allies and corporate partners.

The entire strategy has not been released, but several U.S. officials described it on condition of anonymity. Many aspects of it have been made public by U.S. officials, including Deputy Defense Secretary William Lynn, in speeches over the past several months.

The Pentagon is expected to announce the entire strategy soon.

As an example, the new White House guidelines would allow the military to transmit computer code to another country's network to test the route and make sure connections work -- much like using satellites to take pictures of a location to scout out missile sites or other military capabilities.

The digital code would be passive and could not include a virus or worm that could be triggered to do harm at a later date. But if the U.S. ever got involved in a conflict with that country, the code would have mapped out a path for any offensive cyberattack to take, if approved by the president.

The guidelines also make clear that when under attack, the U.S. can defend itself by blocking cyber intrusions and taking down servers in another country. And, as in cases of mortar or missile
attacks, the U.S. has the right to pursue attackers across national boundaries -- even if those are virtual network lines.

"We must be able to defend and operate freely in cyberspace," Lynn said in a speech last week in Paris. The U.S., he said, must work with other countries to monitor networks and share threat information.

Lynn and others also say the Pentagon must more aggressively protect the networks of defense contractors that possess valuable information about military systems and weapons' designs. In a new pilot program, the Defense Department has begun sharing classified threat intelligence with a handful of companies to help them identify and block malicious cyber activity on their networks.

Over time, Lynn said, the program could be a model for the Homeland Security Department as it works with companies that run critical infrastructure such as power plants, the electric grid and financial systems.

Members of Congress are working on a number of bills to address cybersecurity and have encouraged such public-private partnerships, particularly to secure critical infrastructure. But they also warn of privacy concerns.

"We must institute strict oversight to ensure that no personal communications or sensitive data are inappropriately shared with the government by businesses," said Rep. Jim Langevin, D-R.I., who served as co-chairman of the Center for Strategic and International Studies' cybersecurity commission.

Cyber security experts and defense officials have varying views of cyber war, but they agree that it will be a part of any future conflict.

At a recent Capitol Hill hearing, incoming Pentagon chief Leon Panetta, the outgoing CIA director, said the U.S. must be aggressive in offensive and defensive countermeasures.

"I've often said that there's a strong likelihood that the next Pearl Harbor that we confront could very well be a cyberattack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems," he said.

Stewart Baker, a former Homeland Security official, said Americans need to come to grips with the idea that cyber warfare could hit the U.S. homeland.

"We've had 50 years in which we haven't really had to rethink what might happen in a war here," he said. "We need to think very hard about an actual strategy about how to win a war in which cyber weapons are prominently featured."

Part of that thinking, Baker said, involves ensuring that the U.S. has strong firewalls to prevent attacks and that there are established routes into the networks of potential enemies. But officials also say that cyber capabilities must be put in perspective.

"It's a decisive weapon, but it's not a super weapon," said Lewis. "It's not a nuclear bomb."

It is, however, a new weapon that hackers, criminals and other nations are honing. Already hackers have breached military networks and weapons programs, including key defense contractor Lockheed Martin.

Military officials have also warned repeatedly of cyberattacks and intrusions coming out of China, Russia and Eastern Europe.
"Regrettably," Lynn said, "few weapons in the history of warfare, once created, have gone unused. For this reason, we must have the capability to defend against the full range of cyber threats."

Lynn predicted that terror groups eventually will learn how to launch crippling cyberattacks. Important questions linger about the role of neutral countries. Hackers routinely route their attacks through networks of innocent computers that could be anywhere, including in the U.S. Often it may be difficult to tell exactly where an attack originated or who did it, although forensic capabilities are steadily improving.

That issue was clear during the cyberattack against Estonia in 2007 that used thousands of infected computers to cripple dozens of government and corporate websites. Estonia has blamed Russia for the attack. But, according to Robert Giesler, the Pentagon's former director of information operations, 17 percent of the computers that attacked Estonia were in the United States. He said the question is: Did the Estonians have the right to attack the U.S. in response, and what responsibility did the U.S. bear?

Under the new Pentagon guidelines, it would be unacceptable to deliberately route a cyberattack through another country if that nation has not given permission -- much like U.S. fighter jets need permission to fly through another nation's airspace.

Broadcast Clip – Navy Cyber Forces
(WVEC ABC NORFOLK 22 JUN 11) Mike Gooding
View Clip (RT: 2:06)
China says no cyber warfare with U.S.

By Don Durfee – Wed Jun 22, 2:28 pm ET

BEIJING (Reuters) – There is no cyber warfare taking place between China and the United States, a senior Chinese official said on Wednesday, after weeks of friction over accusations that China may have launched a string of Internet hacking attacks. The two countries might suffer from cyber attacks, but they were in no way directed by either government, Vice Foreign Minister Cui Tiankai told a small group of foreign reporters ahead of a meeting with U.S. officials in Hawaii this weekend.

"I want to clear something up: there are no contradictions between China and the United States" on the issue of hacking, Cui said.

"Though hackers attack the U.S. Internet and China's Internet, I believe they do not represent any country," he added.

Both countries were in fact already discussing the problem of hacking during their regular strategic consultations, Cui said.

"The international community ought to come up with some rules to prevent this misuse of advanced technology," he added.

State Department spokesman Mark Toner declined to comment on Cui's cyber-war comments, but said the inaugural U.S.-China Asia-Pacific Consultations in Honolulu had a general regional focus and no particular cyber warfare agenda. "My understanding is that it is about the Asia-Pacific region, writ large," he said in Washington. Kurt Campbell, the assistant secretary of state for East Asian and Pacific affairs, would be Cui's counterpart in the talks, he said.

The accusations against China have centred on an intrusion into the security networks of Lockheed Martin Corp and other U.S. military contractors, as well as efforts to gain access to the Google email accounts of U.S. officials and Chinese human rights advocates.

'A MOST PRESSING MATTER'

China has vociferously denied having anything to do with hacking attacks, saying it too is a major victim.
"Internet security is an issue for all countries, and it is a most pressing matter," Cui said.
"Of course, every country has different abilities when it comes to this problem," he added.
"The United States is the most advanced country in the world when it comes to this technology, and we hope they can step up communication and cooperation on this with other countries. We also hope this advanced technology is not used for destructive purposes."
The Internet has become a major bone of contention between Washington and Beijing.
This month, Defense Secretary Robert Gates said Washington was seriously concerned about cyber attacks and was prepared to use force against those it considered an act of war.
The latest friction over hacking could bring Internet policy back to the foreground of U.S.-China relations, reprising tension from last year when the Obama administration took up Google's complaints about hacking and censorship from China.
Google partly pulled out of China after that dispute. Since then, it has lost more share to rival Baidu Inc in China's Internet market.
China, with more than 450 million Internet users, exercises tight control and censorship over the Web at home, and has strengthened its grip in recent months.
In February, overseas Chinese websites, inspired by anti-authoritarian uprisings across the Arab world, called for protests across China, raising Beijing's alarm about dissent and prompting tightened restrictions over the Internet.
China already blocks major foreign social websites such as Facebook and Twitter.
Commerce Secretary Gary Locke, named by President Barack Obama as the next U.S. ambassador to China, said last week that the United States was looking into ways to craft trade countermeasures that treat curbs on Internet commerce as non-tariff barriers to trade.
(Additional reporting by Tabassum Zakaria and Paul Eckert in Washington; writing by Ben Blanchard; editing by Robert Birsel and Mohammad Zargham)
US Building Virtual Internet As Cyberattack Testbed

JUNE 20, 2011 6:05 AM PDT
U.S. building virtual Internet as cyberattack testbed

by Lance Whitney

The U.S. is creating a virtual version of the Internet--this one designed as a testbed to help the nation hone its defenses against cyberattacks, according to Reuters and other sources.

Known as the National Cyber Range, the virtual testbed would be set up by the Defense Advanced Research Projects Agency (DARPA), the same agency that kicked off the Internet itself more than 40 years ago. The new simulated mini-Internet would give Washington the opportunity to carry out virtual cyberwarfare games as a way of testing different scenarios and technologies in response to cyberattacks.

To work on the initial development phase of the new system, defense contractor Lockheed Martin was awarded a $5.4 million contract by DARPA in early 2009. The company has provided its own team of cybertechnology experts to work with DARPA on building the test range. Ironically, Lockheed itself was recently the victim of a cyberattack by hackers who used duplicates of SecurID electronic keys to breach network security.

Another organization involved in the National Cyber Range is Johns Hopkins University's Applied Physics Laboratory, which received a $24.7 million contract in early 2010. The lab has been working on the second phase of the project to build and analyze different prototype ranges for the system. This summer, DARPA will reportedly choose one of the two to operate a prototype of the system over the course of the next year.

One of the goals behind the National Cyber Range will be to create a system of networks and computers that can be rebooted after each simulation so the government can quickly test different cyberattack scenarios. With its cost estimated at $130 million, the system is expected to be operational by the middle of next year, Reuters said.

DARPA did not immediately return CNET’s request for comment.

Recent reports revealed that the U.S. would consider a cyberattack an act of war, potentially inviting a response using conventional military weapons.
Is This the Start of Cyber Warfare?

Computer security: Is this the start of cyberwarfare?

Last year's Stuxnet virus attack represented a new kind of threat to critical infrastructure.

Sharon Weinberger

Just over a year ago, a computer in Iran started repeatedly rebooting itself, seemingly without reason. Suspecting some kind of malicious software (malware), analysts at VirusBlokAda, an antivirus-software company in Minsk, examined the misbehaving machine over the Internet, and soon found that they were right. Disturbingly so: the code they extracted from the Iranian machine proved to be a previously unknown computer virus of unprecedented size and complexity.

On 17 June 2010, VirusBlokAda issued a worldwide alert that set off an international race to track down what came to be known as Stuxnet: the most sophisticated computer malware yet found and the harbinger of a new generation of cyberthreats. Unlike conventional malware, which does its
Is This the Start of Cyber Warfare?

damage only in the virtual world of computers and networks, Stuxnet would turn out to target the software that controls pumps, valves, generators and other industrial machines.

"It was the first time we'd analysed a threat that could cause real-world damage, that could actually cause some machine to break, that might be able to cause an explosion," says Liam O Murchu, chief of security response for the world's largest computer-security firm, Symantec in Mountain View, California.

Stuxnet provided chilling proof that groups or nations could launch a cyberattack against a society's vital infrastructures for water and energy. "We are probably just now entering the era of the cyber arms race," says Mikko Hypponen, chief research officer for F-Secure, an antivirus company based in Helsinki.

Worse yet, the Stuxnet episode has highlighted just how inadequate are society's current defences — and how glaring is the gap in cybersecurity science.

Computer-security firms are competitive in the marketplace, but they generally respond to a threat such as Stuxnet with close collaboration behind the scenes. Soon after VirusBlokAda's alert, for example, Kaspersky Lab in Moscow was working with Microsoft in Redmond, Washington, to hunt down the vulnerabilities that the virus was exploiting in the Windows operating system. (It was Microsoft that coined the name Stuxnet, after one of the files hidden in its code. Technically, Stuxnet was a 'worm', a type of malware that can operate on its own without needing another program to infect. But even experts often call it a 'virus', which has become the generic term for self-replicating malware.)

One of the most ambitious and comprehensive responses was led by Symantec, which kept O Murchu and his worldwide team of experts working on Stuxnet around the clock for three months. One major centre of operations was Symantec's malware lab in Culver City, California, which operates like the digital equivalent of a top-level biological containment facility.
Is This the Start of Cyber Warfare?

A sign on the door warns visitors to leave computers, USB flash drives and smart phones outside: any electronic device that passes through that door, even by mistake, will stay there. Inside the lab, the team began by dropping Stuxnet into a simulated networking environment so that they could safely watch what it did. The sheer size of the virus was staggering: some 15,000 lines of code, representing an estimated 10,000 person hours in software development. Compared with any other virus ever seen, says O Murchu, "it's a huge amount of code".

Equally striking was the sophistication of that code. Stuxnet took advantage of two digital certificates of authenticity stolen from respected companies, and exploited four different 'zero day vulnerabilities' — previously unidentified security holes in Windows that were wide open for hackers to use.

Then there was the virus's behaviour. "Very quickly we realized that it was doing something very unusual," recalls O Murchu. Most notably, Stuxnet was trying to talk to the programmable logic controllers (PLCs) that are used to direct industrial machinery. Stuxnet was very selective, however: although the virus could spread to almost any machine running Windows, the crucial parts of its executable code would become active only if that machine was also running Siemens Step7, one of the many supervisory control and data acquisition (SCADA) systems used to manage industrial processes.
Is This the Start of Cyber Warfare?

Many industrial control systems are never connected to the Internet, precisely to protect them from malware and hostile takeover. That led to another aspect of Stuxnet's sophistication. Like most other malware, it could spread over a network. But it could also covertly install itself on a USB drive. So all it would take was one operator unknowingly plugging an infected memory stick into a control-system computer, and the virus could explode into action (see 'How a virus can cripple a nation').
Murky motives

It still wasn't clear what Stuxnet was supposed to do to the Siemens software. The Symantec team got a clue when it realized that the virus was gathering information about the host computers it had infected, and sending the data back to servers in Malaysia and Denmark — presumably to give the unknown perpetrators a way to update the Stuxnet virus covertly. Identifying the command and control servers didn't allow Symantec to identify the perpetrators, but they were able to convince the Internet service providers to cut off the perpetrators' access, rerouting the traffic from the infected computers back to Symantec so that they could eavesdrop. By watching where the traffic to the servers was coming from, O Murchu says, "we were able to see that the majority of infections were in Iran" — at least 60% of them. In fact, the infections seemed to have been appearing there in waves since 2009.

The obvious inference was that the virus had deliberately been directed against Iran, for reasons as yet unknown. But the Symantec investigators couldn't go much further by themselves. They were extremely knowledgeable about computers and networking, but like most malware-protection teams, they had little or no expertise in PLCs or SCADA systems. "At some point in their analysis they just couldn't make any more sense out of what the purpose of this thing was, because they were not able to experiment with the virus in such a lab environment," says Ralph Langner, a control-system security consultant in Hamburg, Germany.

Langner independently took it upon himself to fill that gap. Over the summer, he and his team began running Stuxnet in a lab environment equipped with Siemens software and industrial control systems, and watching how the virus interacted with PLCs. "We began to see very strange and funny results immediately, and I mean by that within the first day of our lab experiment," he says.

Those PLC results allowed Langner to infer that Stuxnet was a directed attack, seeking out specific software and hardware. In mid-September 2010, he
announced on his blog that the evidence supported the suspicion that Stuxnet had been deliberately directed against Iran. The most likely target, he then believed, was the Bushehr nuclear power plant.

**Industrial sabotage**

Speculative though Langner's statements were, the news media quickly picked up on them and spread the word of a targeted cyberweapon. Over the next few months, however, as Langner and others continued to work with the code, the evidence began to point away from Bushehr and towards a uranium-enrichment facility in Natanz, where thousands of centrifuges were separating the rare but fissionable isotope uranium-235 from the heavier uranium-238. Many Western nations believe that this enrichment effort, which ostensibly provides fuel for nuclear power stations, is actually aimed at producing a nuclear weapon. The malware code, according to Langner and others, was designed to alter the speed of the delicate centrifuges, essentially causing the machines to spin out of control and break.

That interpretation is given credence by reports from the International Atomic Energy Agency (IAEA) in Vienna, which document a precipitous drop in the number of operating centrifuges in 2009, the year that many observers think Stuxnet first infected computers in Iran.

“We are probably just now entering the era of the cyber arms race.”

True, the evidence is circumstantial at best. "We don't know what those machines were doing" when they weren't in operation, cautions Ivanka Barszashka, a Bulgarian physicist who studied Iranian centrifuge performance while she was working with the Federation of American Scientists in Washington DC. "We don't know if they were actually broken or if they were just sitting there." Moreover, the Iranian government has officially denied that Stuxnet destroyed large numbers of centrifuges at Natanz, although it does acknowledge that the infection is widespread in the country. And IAEA inspection reports from late 2010 make it clear that any damage was at most a temporary setback: Iran's enrichment capacity is higher than ever.
Is This the Start of Cyber Warfare?

However, if Natanz was the target, that does suggest an answer to the mystery of who created Stuxnet, and why. Given the knowledge required — including expertise in malware, industrial security and the specific types and configurations of the industrial equipment being targeted — most Stuxnet investigators concluded early on that the perpetrators were backed by a government.

Governments have tried to sabotage foreign nuclear programmes before, says Olli Heinonen, a senior fellow at the Belfer Center for Science and International Affairs at Harvard University in Cambridge, Massachusetts, and former deputy director-general of the IAEA. In the 1980s and 1990s, for example, Western governments orchestrated a campaign to inject faulty parts into the network that Pakistan used to supply nuclear technology to countries such as Iran and North Korea. Intelligence agencies, including the US Central Intelligence Agency, have also made other attempts to sell flawed nuclear designs to would-be proliferators. "Stuxnet," says Heinonen, "is another way to do the same thing."

Langner argues that the government behind Stuxnet is that of the United States, which has both the required expertise in cyberwarfare and a long-standing goal of thwarting Iran's nuclear ambitions. Throughout the summer of 2010, while Langner, Symantec and all the other investigators were vigorously trading ideas and information about Stuxnet, the US Department of Homeland Security maintained a puzzling silence, even though it operates Computer Emergency Readiness Teams (CERTs) created specifically to address cyberthreats. True, the CERT at the Idaho National Laboratory outside Idaho Falls, which operates one of the world's most sophisticated testbeds for industrial control systems, did issue a series of alerts. But the first, on 20 July 2010, came more than a month after the initial warning from Belarus and contained nothing new. Later alerts followed the same pattern: too little, too late. "A delayed clipping service," said Dale Peterson, founder of Digital Bond, a SCADA security firm in Sunrise, Florida, on his blog.

"There is no way that they could have missed this problem, or that this is all a misunderstanding. That's just not possible," says Langner, who believes that
Is This the Start of Cyber Warfare?

the Idaho lab's anaemic response was deliberate, intended to cover up the fact that Stuxnet had been created there.

But even Langner has to admit that the evidence against the United States is purely circumstantial. (The US government itself will neither confirm nor deny the allegation, as is its practice for any discussion of covert activity.) And the evidence against the other frequently mentioned suspect, Israel, is even more so. Symantec, for example, points out that a name embedded in Stuxnet's code, Myrtus, could be a reference to a biblical story about a planned massacre of Jews in Persia. But other investigators say that such claims are beyond tenuous. "There are no facts" about Israel, declares Jeffrey Carr, founder and chief executive of Taia Global, a cybersecurity consulting company in Tysons Corner, Virginia.

The Aftermath

The 'who?' may never be discovered. Active investigation of Stuxnet effectively came to an end in February 2011, when Symantec posted a final update to its definitive report on the virus, including key details about its execution, lines of attack and spread over time. Microsoft had long since patched the security holes that Stuxnet exploited, and all the antivirus companies had updated their customers' digital immune systems with the ability to recognize and shut down Stuxnet on sight. New infections are now rare — although they do still occur, and it will take years before all the computers with access to Siemens controllers are patched.

If Stuxnet itself has ceased to be a serious threat, however, cybersecurity experts continue to worry about the larger vulnerabilities that it exposed. Stuxnet essentially laid out a blueprint for future attackers to learn from and perhaps improve, say many of the investigators who have studied it. "In a way, you did open the Pandora's box by launching this attack," says Langner of his suspicions about the United States. "And it might turn back to you guys eventually."

Cybersecurity experts are ill-prepared for the threat, in part because they lack ties to the people who understand industrial control systems. "We've got
Is This the Start of Cyber Warfare?

actually two very different worlds that traditionally have not communicated all that much," says Eric Byres, co-founder and chief technology officer of Tofino Industrial Security in Lantzville, Canada. He applauds Symantec, Langner and others for reaching across that divide. But the effort required to make those connections substantially delayed the investigation.

The divide extends into university computer-science departments, say Byres, himself an ex-academic. Researchers tend to look at industrial-control security as a technical problem, rather than an issue requiring serious scientific attention, he says. So when graduate students express interest in looking at, say, cryptography and industrial controls, they are told that the subject is not mathematically challenging enough for a dissertation project.

"I'm not aware of any academic researchers who have invested significantly in the study of Stuxnet," agrees Andrew Ginter, director of industrial security for the North American group of Waterfall Security Solutions, based in Tel Aviv, Israel. Almost the only researchers doing that kind of work are in industrial or government settings — among them a team at the Idaho National Laboratory working on a next-generation system called Sophia, which tries to protect industrial control systems against Stuxnet-like threats by detecting anomalies in the network.

One barrier for academics working on cybersecurity is access to the malware that they must protect against. That was not such a problem for Stuxnet itself, because its code was posted on the web shortly after it was first identified. But in general, the careful safeguards that Symantec and other companies put in place in secure labs to protect the escape of malware may also inadvertently be a barrier for researchers who need to study them. "If you're doing research into biological agents, it's limited groups that have them and they are largely unwilling to share; the same holds true for malware," says Anup Ghosh, chief scientist at the Center for Secure Information Systems at George Mason University in Fairfax, Virginia. "To advance the field, researchers need access to good data sets," says Ghosh, who was once a programme manager at the US Defense Advanced Research Projects Agency, and is now working on a malware detector designed to identify viruses on the
basis of how they behave, rather than on specific patterns in their code, known as signatures.

Academic researchers are also inhibited by a certain squeamishness about digital weaponry, according to Herb Lin, chief scientist at the Computer Science and Telecommunications Board of the US National Research Council in Washington DC. He points out that to understand how to guard against cyberattacks, it may help to know how to commit them. Yet teaching graduate students to write malware is "very controversial", he says. "People say, 'What do you mean: you're training hackers?'"

Preparing for the next attack

A study last year by the JASON group, which advises the US government on science and technology matters, including defence, found broad challenges for cybersecurity (JASON Science of Cyber-Security; MITRE Corporation, 2010). Perhaps most important was its conclusion that the field was "underdeveloped in reporting experimental results, and consequently in the ability to use them".

Roy Maxion, a computer scientist at Carnegie Mellon University in Pittsburgh, Pennsylvania, who briefed JASON, goes further, saying that cybersecurity suffers from a lack of scientific rigour. Medical professionals over the past 200 years transformed themselves from purveyors of leeches to modern scientists with the advent of evidence-based medicine, he notes. "In computer science and in computer security in particular, that train is nowhere in sight."

Computer science has developed largely as a collection of what Maxion calls "clever parlour tricks". For example, at one conference, the leading paper showed how researchers could read computer screens by looking at the reflections off windows and other objects. "From a practical point of view, anyone in a classified meeting would go, 'pooh',' he says. "In places where they don't want you to know [what's on the computer screen], there are no windows. Yet, that was the buzz that year."

Maxion sees an urgent need for computer-science and security curricula to
Is This the Start of Cyber Warfare?

include courses in traditional research methods, such as experimental design and statistics — none of which is currently required. "Why does it matter?" he asks. "Because we don't have a scientific basis for investigating phenomena like Stuxnet, or the kind of defences that would be effective against it."

Also troubling for many of the Stuxnet investigators was the US government's lacklustre response to the virus (assuming that it was not the perpetrator). Stuxnet represents a new generation of cyberweapon that could be turned against US targets, but there is no evidence that the government is making the obvious preparations for such an attack — for example, plans for a coordinated response that pools resources from academia, research institutes and private business.

Other countries seem to be taking the threat more seriously. Some of China's universities and vocational colleges have reportedly forged strong connections with the military to work on cybersecurity, for example. And Israel also seems to be exploiting its computing expertise for national security. A few months before the discovery of Stuxnet, Yuval Elovici, a computer scientist and director of Deutsche Telekom Laboratories at Ben-Gurion University of the Negev in Beersheba, Israel, told Nature that he was working closely with the country's Ministry of Defense on cybersecurity. He presciently warned that the next wave of cyberattacks would be aimed at physical infrastructures. "What would happen if there were a code injection into SCADA? What if someone would activate it suddenly?" Elovici asked. He and other experts have been warning for several years now that such an attack on SCADA systems controlling the electricity grid could spark nationwide blackouts, or that the safety systems of power plants could be overridden, causing a shutdown or a serious accident. Similar disruptions could hit water and sewage systems, or even food processing plants.

Such attacks, Elovici warned, are both realistic and underestimated. Asked how bad one would be, Elovici was unequivocal. "I think," he said, "it would be much stronger than the impact of setting several atomic bombs on major cities."
Is This the Start of Cyber Warfare?
Navy Must Cut IT Business Systems Spending by 25%

Navy Must Cut IT Business Systems Spending By 25 Percent
(FEDERAL NEWS RADIO 10 JUN 11) ... Jared Serbu

Faced with the challenge of finding substantial savings in its technology budget, the Department of the Navy (DON) is turning to industry for ideas on potentially cheaper alternatives to high-cost IT items such as email and data storage.

Terry Halvorsen, the Navy Department's chief information officer announced earlier that he expected that he's been told to find "significant" savings in the department's business IT systems. The goal is to cut business systems and preserve technological capabilities for warfighting in the face of anticipated Defense-wide budget reductions.

On Thursday, Robert Work, the Navy Department's undersecretary, put some proportion to those savings when he told an AFCEA conference he had ordered Halverson to reduce IT spending on Navy and Marine Corps business systems by 25 percent over the course of DoD's five-year defense spending plan.

"You don't get 25 percent by doing what you're doing more efficiently," Halverson said. "We have to change the model of the way we are doing business."

Consequently, there are commercial ideas the department has new interests in. He said the Navy will soon issue requests for information (RFIs) to industry on several topics, including data hosting and commercial enterprise email.

"That means we might be willing to have a discussion that says a private email provider could provide us with our email and our email storage capability, if they could provide it with the minimum security capabilities that we need," he said.

Halvorsen said the service also would have to be hosted entirely within the continental United States, and host only the email traffic on the unclassified network, known as NIPRNet, which he said accounted for the vast majority of costs.

"One of the things you have to do if you're going to get money is follow money. You have to go where you're spending your money, and we spend a lot more of our money on the unclassified side of things, so that's what we're going to look at first," he said. "Having that email would do a couple of things. Immediately, it could save us some direct money. It could also increase access. One of the things that would be nice is if everybody in the department didn't have to have extra devices just to get to their email."

A second RFI would deal with data storage. Halvorsen said they're exploring the idea of public-private partnerships on Navy and Marine Corps bases, modeled after the way DoD privatized on-base housing for military families.

"Maybe it's possible for us to say to some private company, 'You can build a data center on our base. We will provide all the security, the physical, the virtual, and we'll be your subcontractor for security. If you get it right, you can even use that data center for non-DON business.' Is that doable? I don't know yet. Is it explorable? Yes," he said.

Halvorsen said he's already had some one-on-one talks with industry that led him to conclude there are savings to be had in such a partnership if they can work past security, policy and other
Navy Must Cut IT Business Systems Spending by 25%

concerns. He said his guess is the department will wind up with a federated system of data centers, with some operated by the Navy, some by the Marines, some by the private sector and some by other DoD entities such as the Defense Information Systems Agency.

But unlike the Army, which is in the middle of migrating all of its email users to a DISA cloud, Halvorsen said the Navy doesn't see DISA as a good choice for email, at least for now.

"We encourage the Army and DISA to keep working it, but they're in the beginning stages of an enterprise email capability that we already enjoy," he said. "Frankly, where they're at right now, I'd get less capability for more money. As soon as they get to a point where they can deliver as much capability as we have for less money, we'll be there."

Undersecretary Work said the DON is targeting its business systems for efficiency savings because they're the ones the Navy and Marine Corps can afford to take some level of experimental risks with, unlike systems service members rely on directly in the battle space.

But, Work said, the overall IT spending picture for the Navy and Marine Corps will probably fare relatively well when other systems are included.

"Battle networks are central in the guided munitions regime," he said. "That is why the United States is so dominant in conventional warfare, and with the proliferation of guided weapons, battle networks will be central in the future. And cyber warfare is a growth area. We're debating right now whether to make the Navy cyber command its own budget-submitting organization, which should give you an idea of how important we think this is."

Listen To Audio (RT: 5:19)
Navy goes full speed ahead with next-gen IT projects

Program managers report progress with CANES, NGEN

By Amber Corrin
Jun 10, 2011

The Navy is pushing ahead with two of its most visible IT programs, the Consolidated Afloat Networks and Enterprise Services (CANES) and the land-based Next Generation Enterprise Network (NGEN). Officials are hopeful the programs will help revolutionize naval IT, and the programs also are gearing up for contract action.

“This is the only way we can afford to modernize everything we need to, all the legacy networks, but we have to be careful not to break anything or let anything fall through the cracks,” said Capt. D.J. LeGoff, program manager, Tactical Networks Program Office. LeGoff discussed CANES as part of a Navy Program Executive Office panel at AFCEA Naval IT Day on June 9 in Vienna, Va.

“We cannot keep paying those kinds of dollars to support legacy systems,” LeGoff said.

CANES is designed to be interoperable with the Navy-Marine Corps Intranet (NMCI), the legacy predecessor to NGEN, which is slated for April 2014 completion, according to Capt. Shawn Hendricks, program manager, Naval Enterprise Networks Program Office.

Brig. Gen. Kevin Nally, Marine Corps CIO and director for command, control, communications and computers, said that some NMCI accounts have already successfully begun transitioning to the NGEN test bed.

Requests for proposals for NGEN will begin release this summer, with initial components of the RFP coming on June 30, July 30 and Aug. 30. The final draft will come out Sept. 30 and final RFPs will be out by Dec. 21, Hendricks said.

All contracts will be awarded no later than December 2012, with the systems
Navy Goes Full Speed Ahead With Next-Gen IT Projects

engineering technical review set for completion no later than May 2013 and transition complete no later than April 30, 2014, he said.

A just-released NGEN technical data synopsis is available on fbo.gov. Hendricks said those interested in more information should monitor the FedBizOpps website.

The major transitions of both CANES and NGEN won’t be without challenges, Hendricks and LeGoff both said.

“The budget realities mean that we have to find efficiencies within our own infrastructure,” said LeGoff, adding that consolidation and reduction as well as configuration management and training also present challenges of their own.

Hendricks also noted that budget issues will be tough but necessary to overcome, stating that despite an expected decrease in funding, capabilities must be maintained and productivity must be increased.
As if all the millions of dollars and untold effort the Navy spends on networks and IT systems weren’t enough to underline their importance, top service officials decided it was time to be more direct about that key role as they prepare to make some tough choices.

For the Navy, IT does not simply support infrastructure — it is a combat system, said Adm. Jonathan Greenert, vice chief of naval operations, in a keynote address at AFCEA's Naval IT Day earlier this month.

Unfortunately, it’s a combat system that has become bloated, inefficient and vulnerable, other Navy officials said during the conference, which Henry Kenyon and Amber Corrin covered for Federal Computer Week's sister publication Defense Systems. The Navy wants to fix those shortcomings, but it will take a significant effort to realign its operations and culture to support recognition of IT as a combat system.

The to-do list is long and growing as the Navy deploys new IT-centric capabilities, such as unmanned aerial vehicles (UAVs) and stouter cyber defenses. A tight fiscal climate and increasing pressure to downsize greatly complicate the task. The Navy is in the middle of a strategic review of all its operations as it looks for opportunities to pare unneeded programs and focus limited funds on critical and high-growth areas. The stakes are high.

“We are going to make decisions in the next two years that will set the stage for the [Defense Department] for the next 10 years or more,” Undersecretary of the Navy Robert Work said at the conference.

Navy officials realize they must make the most of every dollar they spend on basic IT infrastructure so they have sufficient funds to support future capabilities. To that end, they are exploring the possibility of using commercial cloud services for e-mail and data storage.

“If our security standards can be met,...maybe [commercial services] are options,” said Navy Department CIO Terry Halvorsen. He also said officials are keeping an eye on the joint enterprise e-mail effort under way between the Army and the Defense Information Systems Agency to see if it could deliver a more affordable messaging option for the Navy.

Meanwhile, new capabilities such as UAVs and remote sensors are producing a flood of data and straining the Navy’s IT infrastructure, resulting in a 1,000 percent increase in afloat bandwidth demand, said Dave Weddel, assistant deputy chief of naval operations for information dominance. The challenge is not only to acquire and process that data, but also to share and act on it.

None of that will be possible if the underlying infrastructure is not adequately secured. Along those lines, the Navy is preparing to launch initial operations at four new Regional Network Operations and Security Centers that will support the Navy's Fleet Cyber Command.

“These [centers] will combine network operations with computer network defense” and will exploit the adversary, predict future attacks and defend networks, said Rear Adm. Edward Deets III, commander of the Naval Network Warfare Command.

In addition, as part of its Cyber Asset Reduction and Security effort, the Navy is working to...
reduce its network portfolio by 51 percent and has already eliminated nearly 1,000 networks, 20,000 servers and more than 32,000 devices.

“The fewer number of networks we’re attempting to secure out there, the better,” Deets said. “We’ve tremendously reduced our vulnerability.”
HP Orders Worth $1 Billion At Risk As Navy Takes Over Intranet

(BLOOMBERG NEWS 23 JUN 11) ... Nick Taborek

Hewlett-Packard Co. is at risk of losing more than $1 billion a year in federal business as the U.S. Navy assumes management responsibility for its internal communications network.

The Navy and Marine Corps contract has been Palo Alto, California-based HP's largest services program since 2008, contributing $1.1 billion in company revenue in 2009, according to data compiled by Bloomberg Government. HP had revenue of $126 billion in the year ended Oct. 31.

The Navy, which operates the world's largest Intranet with 700,000 users, plans to replace HP's contract with five awards as it begins an effort to cut business technology costs by 25 percent. Companies will have to compete more frequently to keep the work, which the Navy will begin awarding next year under the Next Generation Enterprise Network, or NGEN, program.

"The work is being taken away from Hewlett Packard and doled out," said Loren Thompson, chief operating officer of the Lexington Institute, a think tank in Arlington, Virginia. "Many companies in the defense IT sector could benefit."

Raytheon Co. last year had the most Navy information-technology sales with $2.24 billion. Lockheed Martin Corp. was the second-biggest provider with $1.87 billion, according to Bloomberg data.

HP in 2008 acquired Electronic Data Systems, a Plano, Texas, company founded by Ross Perot that in 2000 became the network integrator for the Navy and Marine Corps. The contract brought $9.5 billion in revenue in 10 years, according to Bloomberg data. HP won a $3.4 billion award last year to supply the services until the transition to NGEN is completed in 2014.

Painful Years

"Those early years were painful, for both the Navy and EDS," said Ray Bjorklund, chief knowledge officer at Deltek Information Solutions, based in Herndon, Virginia.

The Navy and Marine Corps network got low marks from users and met just three of 20 "performance targets" in a 2006 review by the Government Accountability Office.

HP remains a "key player" in the competition and "could get very nearly the same amount of work" under NGEN as it had previously, Bjorklund said.

The Navy plans to spend $1.7 billion on the program next fiscal year, according to budget documents. The first two requests for proposals, for "transport services" and "enterprise services" including e-mail and data storage, will be released by Dec. 21 and will make up "the lion's share" of NGEN spending, said Shawn Hendricks, program manager for the Naval Enterprise Network.

HP Response

"Forcing the next generation of IT services into a segmented contracting model risks increased costs, and worse, loss of operational security and efficiency," said Bill Toti, HP's vice president for
HP Orders Worth $1 Billion At Risk As Navy Takes Over Intranet

U.S. Navy Strategic Programs.

HP will compete for the work, Toti said in a telephone interview. "We bring the knowledge as the ones that crafted the system they're operating now."

To prevail, HP will have to fend off rivals including Harris IT Services, a unit of Melbourne, Florida-based Harris Corp. that is among the more than 100 subcontractors on the Navy and Marine contract. Harris became involved in the program in 2007 when it acquired subcontractor MultiMax Inc.

HP "essentially provides everything" and makes all recommendations to the Navy about which services and products to use, Cynthia Gagnon, Harris's director of capture management, said in a June 20 phone interview.

Subcontractors are "looking forward to more open competition and greater access to the customer," she said.

Harris is leading a team made up of Computer Sciences Corp. and General Dynamics Corp., both based in Falls Church, Virginia, and San Jose, California-based Cisco Systems Inc. in a bid for the transport-services contract. The company is also part of a team that may bid on the enterprise-services contract.

Navy Oversight

The Navy will take responsibility for integrating the work of its contractors, a management role previously handled by HP.

The GAO says the approach may add as much as $5.3 billion to the Navy's five-year IT tab. The Navy's acquisition strategy involves "greater schedule and performance risks" tied to its more complex management responsibility overseeing multiple contracts, according to a March report from the audit agency.

Dividing the information-technology work into five segments lets the Navy hold more frequent competitions that will allow the service to take advantage of innovation, the Navy's Hendricks said. The other three contracts under NGEN are for hardware, software licenses and network security.

The transport and enterprise services contracts will probably be for one year with optional single-year renewals, Hendricks said. By comparison, EDS's original Navy and Marine Corps contract lasted for 10 years and was extended an additional 43 months without competition.
The Army's big network experiment

By Philip Ewing Tuesday, June 14th, 2011 4:00 pm

The Army has high hopes for what it'll learn from its big network exercise now underway down at White Sands, N.M. About 3,800 soldiers are using the handheld devices you’ve read about here on Buzz, as well as the new Joint Tactical Radio System, the Mounted Soldier System, and a whole smorgasbord of other types of equipment, said Army spokesman Paul Mehney. But the service isn’t just testing all this equipment to see how it works — which it is — the brass also want to learn as much as it can about how soldiers actually use it, Mehney said.

One of the things that has made the digital era so unpredictable, maddening and exhilarating is that when a population gets enough computers or mobile devices, users begin doing things designers either didn’t intend or didn’t expect. As the Army begins to make its networks more robust, and give more toys to more people across the battlefield, it isn’t like fielding a new bullet or a new pair of boots. With a mobile phone or a tablet computer connected to a brigade-sized network, a soldier or a unit can theoretically collaborate in new ways, get more information from higher headquarters, and also push more information back up to commanders to help them make decisions. What the Army wants to see is how exactly all those things come together.

Mehney gave one example: Soldiers might be able to use their mobile devices to take a photo of someone they suspect could be a high-value target, then quickly send the image to an intelligence officer to confirm it’s the right guy. If they’ve detained the wrong person, they can let him go without the need to drag him all the way back to base. Or suppose a convoy in unfamiliar territory could get a warning on their screens that they’re entering an area where other units have been ambushed or hit by IEDs.

Soldiers also tell Army officials what they don’t like about their high-tech toys. In an exercise last year, Mehney said, Army program officials were eager for troops to use a set of small unmanned sensors to watch remote parts of the battlefield; the sensors could take pictures of bad guys and alert commanders where they were. “But the soldiers came back and said, ‘yeah, we’ve got this capability, but we hardly use it,” he said. “We don’t care about the sensors — half the information is stagnant when we get it anyway. What we want is the ability to collaborate using this little laptop.”

Troops liked the ability to get charts, operational data and other information on a networked, mobile laptop as part of the Incremental Battle Command Extension — IBEX — so the troops have them again at this year’s exercise at White Sands.

But the Army won’t always have the luxury of operating within range of commercial
mobile networks, as in New Mexico. Will units have to rely on local networks, or take their own communications infrastructure into battle to be sure they can get everyone connected? The Army doesn’t know yet, Mehney said. One of the things service officials are hoping to learn from the White Sands exercise is which of those directions to go — or to prepare for both.

"It’s important to note this is not an end-all activity," he said. “This is just the beginning of this process for the Army.”
It’s one of Defense Secretary Robert Gates’ lasting legacies: pumping billions into producing drones, cameras, sensors and aerostats so U.S. troops can have a better picture of the wars they fight. And the Office of Naval Research is saying it’s still not good enough.

Not that the office is criticizing Gates. It’s just that a new solicitation from the Navy’s super-scientists to create a big new “autonomous persistent tactical surveillance” system is really impatient with all the inefficiencies that confront troops starved for better intelligence, surveillance and reconnaissance tools. And no wonder: The program’s out-there goal is no less than “measuring the value of information across an area as a function of time given knowledge of current and future missions and to measure the amount of known relevant information spatially organized as a function of time.”

The basic idea behind Autonomous Persistent Tactical Surveillance is to link collected intelligence into the command-and-control systems that let small units talk to their headquarters. That should better allow “sensor and data analysis nodes to anticipate the information needs of the tactical warfighter.” That linkup could work in a secured cloud which mobile handsets should be able to access, providing “simultaneous situational awareness” to a Marine squad and its command center. Eat your heart out, Army smartphone program.

That’s not all. The program wants to expand the Navy’s aperture, using “coverage history, data and context from available sources” to get a persistent fix on a huge area of space — “typically 40 nmi [nautical miles] by 40 nmi.” (Eat your heart out, Air Force "Blue Devil" super-blimp. Gorgon Stare, you might have a rival.) That should knit
Navy: Actually, Most Military Intel Systems Suck

together into an “autonomous sensing system” thanks to a variety of unmanned vehicles “operating in autonomous mode.”

So think networked drones working in concert to get a long-term view on a massive area, “deciding” what’s relevant to a small Marine unit by “anticipating” its mission requirements, all linked to headquarters, and discarding information that’s either perishable or useless. Darpa wants to create a thinking camera. This is a step beyond.

To get a sense of why the Navy thinks it’s necessary to upgrade the military’s arsenal of cameras, sensors and drones, the solicitation basically itemizes all their shortcomings — at excruciating length.

They don’t weight the relative importance of collected information to specific missions, or indicate to analysts what info is perishable. They don’t use “unified information ontologies or data mappings,” and a snapshot that lacks “space-time and geocultural context” isn’t of much use. They can’t “assess large quantities of imagery and full motion video information and determine potential threat activities using algorithms that work with limited IT assets.”

They can’t be a voice for the small unit commander, channelling his or her needs up to the higher headquarters that controls a drone or a satellite. They can’t “project the value of information versus location given mission plans and area events over time.” And they can’t “align tactical and strategic analysis capabilities and sensor resources to current and future information requirements.”

Aside from that, military intelligence, surveillance and reconnaissance is working great.

The Office of Naval Research didn’t make anyone available to discuss Autonomous Persistent Tactical Surveillance, and demurred from further comment since the
solicitation is a long way from being awarded. Whether this actually gets seen through to completion is a separate question. Many, many problems have vexed similarly ambitious surveillance platforms. And this looks to be one of the most ambitious of all.
DISA Eyes Central Management of 1 Million Cell Phones and Other Wireless Devices

DISA eyes central management of 1 million cellphones and other wireless devices
BY BOB BREWIN 06/13/2011
The Defense Information Systems Agency has bold plans to centrally manage and monitor 1 million cellphones and other mobile gadgets Defense Department personnel use. It wants industry to provide suggestions for how to do so by June 20.

In a request for information released in May, DISA said it wants to establish itself as a mobile virtual network operator, an entity that leases bandwidth from mobile carriers and then resells it.

DISA said it wants to use the MVNO structure, which is widely used in Europe, to better manage cellphones and to monitor their security "while minimizing the overall attack surface exposed to adversaries."

In addition, DISA said it wants to extend this management structure to include smartphones, tablet computers and Wi-Fi access. To plug cellular coverage gaps, the agency would consider using the contract to deploy low-power, short-range transmitters know as femtocells, typically used in homes or small business, or picocells, used in office buildings, malls, airports and train stations that lack full coverage from cellular carrier base stations and towers.

The MVNO would centrally manage the subscriber identity module cards -- chips that include the phone numbers and security modules, including encryption keys -- and would give DISA the ability to block phones or other mobile devices from accessing the mobile network.

The network managed by the MVNO would feature an always-on VPN and would include dedicated links to government centers handling the mobile phones and other gadgets, DISA said.

Currently, Defense does not have a central cellphone services contract. The Pentagon, military services and even individual commands negotiate separate contracts. Cellular service for personnel stationed in the Pentagon, for example, is provided by Defense Telecommunications Services-Washington, which has contacts with AT&T, Sprint, T-Mobile and Verizon Wireless for domestic service and Cellhire for international service.

The Navy has its own separate contracts with the four domestic carriers as well as with the Army and Air Force.

Bernie Skoch, a telecommunications consultant and retired Air Force brigadier general with extensive telecommunications experience, said it makes sense for DISA to want to centrally manage its mobile phones and computers, with increased security being the real payoff.
DISA Eyes Central Management of 1 Million Cell Phones and Other Wireless Devices

DISA said it views any potential MVNO contract as a "niche telecom business" that would provide service to Defense, along with other federal agencies, and state and local governments. Skoch agreed, and pegged the value of the MVNO contract at $10 million.

Marlin Forbes, former Defense vice president for Verizon, estimated the value of the underlying cellular contracts managed by the MVNO would be at least $50 million a month, assuming a modest $50 a month bill per phone for 1 million phones.

Forbes said DISA faces a daunting task in managing cellular phones globally. "I don't know anyone who can do that today" in myriad countries where Defense personnel are stationed, he said.
The Defense Information Systems Agency (DISA) is stepping up its effort to make U.S. Defense Department computer networks more accessible to users, specifically on mobile devices.

"Technological advances and calculated investments will ensure our joint forces have reliable access to the right information at the right time, from any device anywhere in the world," the agency stated in its 2011-12 campaign plan released June 20.

The document guides the agency's budget planning and lays out its priorities.

DISA also plans to "focus on the maturation and migrations" to cloud computing and server virtualization. Cloud computing is the storage of data on remote servers that are easily accessible from a multitude of devices.

"Technological enhancements are necessary to implement a full cloud computing strategy, including enhanced information assurance capabilities, improved application monitoring, automated provisioning, and automated infrastructure orchestration," the report states. "DISA must deploy innovative capabilities and influence research community investments in DoD's technology priorities, including cross domain solutions, data replication and synchronization, and authentication and authorization."

To that end, the agency is working to deliver mobile computing applications, including capabilities that visualize mission information. DISA is also working infrastructure needed to support these types of systems.

"Advances in mobile computing technologies offer significant and unprecedented opportunities for seamless information sharing to end users," the campaign plan
DISA Promotes Remote Access for DoD Computers

states.

As for acquisition, the agency plans to "use small incremental releases which build on previous functionality for deployment of software capabilities and services," the document states.

The agency also wants to "evolve the acquisition process to support a predominately agile development process" and "provide a flexible, extensible agency framework, supported by the appropriate tools and processes, to facilitate the rapid development and deployment of capabilities," the campaign plan states.

In the contracting business, DISA wants to "improve the timeliness and quality of contracting by optimizing processes and systems for efficiency guided by metrics and effective contract oversight."

Additionally, the agency wants to implement "enterprise-focused contracting activities capable of proactively meeting customer requirements and expectations."
U.S. Cyber Command's concept of operations lacks detail and clarity around roles and responsibilities that enable CYBERCOM's support for Defense Department cyberspace operations, say military officials.

Officials from the four military services requested greater specificity around command and control relationships for cyberspace operations, being led by CYBERCOM, and geographic combatant commands, says the Government Accountability Office.

"According to its Concept of Operations, when a cyberspace operation is confined to the area of responsibility of one geographic combatant command, U.S. Cyber Command will act as a supporting commander to the geographic combatant commander. When the cyberspace operations impact global functions or create effects across the borders of more than one geographic combatant command's area of responsibility, the geographic combatant commanders may support U.S. Cyber Command, as directed," states a GAO report (.pdf) released publically June 20 but dated May 2011.

However, there are several different models for such support relationships and the operations document does not identify a specific model for CYBERCOM and the geographic combatant commands to follow.

The Joint Chiefs of Staff has been working since September 2009 on a document to accompany the concept of operations, but it's still a draft, according to report authors. In addition to creating a more "comprehensive doctrine," DoD should also establish common definitions for cyberspace operations, advises GAO.

Officials at military services also told GAO auditors they have not received guidance from CYBERCOM regarding longterm personnel requirements and capabilities. As such, each branch is developing internal protocol, "moving forward using disparate, service-specific approaches to operationalizing cyberspace," says the report. DoD is also reviewing the appropriate roles for government civilians and military personnel in the cyber domain as current policy guidance is insufficient, the report says.

In a written response to GAO, DoD agreed with the analysis and recommendations, saying it is taking action to address these issues internally and achieving them is
CYBERCOM, Geographic Combatant Command Roles Unclear, Finds GAO

"highly desirable."

For more:
- see the report GAO-11-421 (.pdf)
Navy To Make Downselect Decision For CANES Prime Contractor By December

(DEFENSE DAILY 24 JUN 11) ... Carlo Munoz

SAN DIEGO-- Industry officials competing for the Navy’s next generation ship-to-ship communication system anticipate service officials to issue a downselect decision to a prime contractor for the program in December.

The downselect decision between Northrop Grumman [NOC] and Lockheed Martin [LMT] for the Navy’s Consolidated Afloat Networks and Enterprise Services (CANES) program will also coincide with the system design and development (SDD) milestone also set for December, Dave Wegmann, CANES program manager for Northrop Grumman, said after a June 10 briefing here.

The tactical networks division (PMW160) within the Navy’s Program Executive Office for Command, Control, Communications, Computers and Intelligence at Space and Naval Systems Command (SPAWAR), will oversee both the downselect and SDD milestone.

If successful, the Northrop Grumman team hopes to complete the first installation of their version of CANES aboard a Navy destroyer by fiscal year 2012, Wegmann said. Program officials have already developed and are in the process of testing a prototype version of the system at their San Diego facilities.

Last March, the Navy issued separate development contracts to Northrop Grumman and Lockheed Martin to develop CANES for the Navy’s surface fleet. Since then, SPAWAR officials granted the Northrop Grumman-built system critical design review (CDR) approval last month. The Navy has yet to complete its review of the Lockheed Martin variant, Wegmann said.

As both CANES teams work toward that December deadline, a new open system development strategy should give the company an edge during the downselect process, Wegmann said. That strategy, known as the Modular Open Systems Approach–Competitive (MOSA-C) was developed by Northrop Grumman engineers specifically for the CANES competition, according to Wegmann.

While defense industry firms have been heavily integrating commercial off-the-shelf technologies into military systems for decades, “the reality is that the [Pentagon] acquisition community has not reaped the benefits of COTS, from a cost perspective, as much as we think they should be,” he said.

The fact is that once all the modifications needed to make COTS hardware and software battle ready are complete, the additional cost associated with that work nearly negates any cost savings associated with using COTS to begin with, he explained.

“So the combination of those...factors, when the government goes to recompete a contract, it is no longer truly COTS,” he said. “You have now got this proprietary stuff and it gets very difficult to compete.”

By implementing its MOSA-C strategy into the CANES competition, which is COTS –heavy as well as open architecture based, company officials believe it can provide a combat-ready system while retaining cost savings goals.

“We felt CANES was an opportunity to really partner with the government to provide a truly
open system, both logically and physically,” he said. “We developed a process to achieve those goals.”

Using the CANES program requirements, developed by the Navy’s Program Executive Office for Command, Control, Communications, Computers and Intelligence within Space and Naval Systems Command (SPAWAR), company officials determined the entire system could be stood up on COTS systems and applications.

That said, Northrop Grumman officials were able to draft “a requirements-based flow down into components and functions...and describe the capabilities that you can trace all the way up [to] the requirements, [and] all way down to a physical component” for CANES hardware and software.

With the specific components identified, company officials can then compete the different pieces of the system among various subcontractors, to drive down cost and provide best value, he said.

Under the MOSA-C approach, Northrop Grumman can then pick the best of breed from those subcontractor offers, and guarantee those components can “plug-and-play” into that overarching, open-source architecture--while ensuring the subcomponents fall in line with Navy specs.
DoD must unify maritime domain awareness efforts, says GAO

June 23, 2011 — 12:08pm ET | By Molly Bernhart Walker

The Defense Department lacks a departmentwide strategy for maritime domain awareness and without one, it cannot chart performance, assess risk or prioritize resource allocation for intelligence, surveillance and reconnaissance, reports the Government Accountability Office.

"It is important that DoD components' efforts are consolidated together and aligned amongst each other to ensure that departmentwide maritime domain awareness needs are met and appropriate contributions to the efforts of its interagency partners are made," say auditors in a GAO report (.pdf) published June 20.

Currently, DoD components prioritize maritime domain awareness risks on a mission-by-mission basis, says GAO.

While DoD acknowledges that there are maritime domain awareness capability gaps in its four different strategy documents that mention the problem, none of the documents fully address organizational roles and responsibilities, say auditors. The national and DoD strategy documents also lack provisions for allocating resources, measuring performance and monitoring progress, says GAO.

GAO recommends DoD develop and implement a departmentwide maritime domain awareness strategy and undertake a comprehensive risk-based analysis, according to the report. In a response to the report, DoD agreed with GAO's analysis and outlined action, planned or currently underway, to address the problems.

Maritime domain awareness challenges vary depending on location. For example, Navy lists piracy as an issue off the west African coast, trade disruption in the waters east of the Indian subcontinent and human smuggling as a problem near the West Coast of the United States, according to GAO.

For more:
- see the report, GAO-11-621 (.pdf)
The Senate just drove a stake into the Navy’s high-tech heart. The directed energy and electromagnetic weapons intended to protect the surface ships of the future? Terminated.

The Free Electron Laser and the Electromagnetic Rail Gun are experimental weapons that the Navy hope will one day burn missiles careening toward their ships out of the sky and fire bullets at hypersonic speeds at targets thousands of miles away. Neither will be ready until at least the 2020s, the Navy estimates. But the Senate Armed Services Committee has a better delivery date in mind: never.

The committee approved its version of the fiscal 2012 defense authorization bill on Friday, priced to move at $664.5 billion, some $6.4 billion less than what the Obama administration wanted. The bill “terminates” the Free Electron Laser and the rail gun, a summary released by the committee gleefully reports.

“The determination was that the Free Electron Laser has the highest technical risk in terms of being ultimately able to field on a ship, so we thought the Navy could better concentrate on other laser programs,” explains Rick DeBobes, the chief of staff for the committee. “With the Electromagnetic Rail Gun, the committee felt the technical
challenges to developing and fielding the weapon would be daunting, particularly [related to] the power required and the barrel of the gun having limited life."

Both weapons are apples in the eye of the Office of Naval Research, the mad scientists of the Navy. “We’re fast approaching the limits of our ability to hit maneuvering pieces of metal in the sky with other maneuvering pieces of metal,” its leader, Rear Adm. Nevin Carr, told me in February. The answer, he thinks, is hypersonics and directed energy weapons, hastening “the end of the dominance of the missile,” Adm. Gary Roughead, the top officer in the Navy, told me last month. With China developing carrier-killer missiles and smaller missiles proliferating widely, both weapons would allow the Navy to blunt the missile threat and attack adversaries from vast distances.

And both have recently experienced technical milestones that made researchers squeal with glee.

In December, the Navy corralled reporters to Dahlgren, Virginia, to watch a rail gun the size of a schoolbus fire a 23-pound bullet using no moving parts — just 33 megajoules of energy, a world record. (A prototype of a ship-ready rail gun is pictured above.)

And this winter, the Free Electron Laser, the most powerful and sophisticated laser there is, boasted two big advances within a month. In January, its 14-kilowatt prototype passed tests that injected enough energy into it to get it up to a megawatt’s worth of death ray — a “remarkable breakthrough,” nine months ahead of schedule, the Office of Naval Research crowed. The next month, its testers at the Jefferson Lab in Newport News added even more power. Researchers think it could be far more than a weapon: it might act as a super-sensor, and Yale scientists use it to hunt for cosmic energy.

Shipboard power is the question mark surrounding both weapons. The laser and the rail gun require diverting power from a ship’s generators in order to fire. The Navy’s
waved that away, saying that its onboard generators — especially the superpowerful ones in development — can handle the megawattage necessary, and the Free Electron Laser’s guts are shaped like a racetrack to “recycle” some of the energy injected into it. But both plans rely on the power efficiency of ships that aren’t built yet.

Neither comes cheap, either. The Navy’s spent some $211 million since 2005 developing the rail gun. Its milestones with the Free Electron Laser — in development in some form since the ’90s — led it to ask Congress for $60 million in annual directed-energy research funds, most of which go to the superlaser. Needless to say, a Senate panel facing a huge budget crunch was unsympathetic.

The Office of Naval Research didn’t respond by press time. The process of passing a defense budget making it through no fewer than four committees and two floor votes, so it’s not like these programs cease to exist. But unless the Navy makes a big push for its futuristic weapons, both of them will die on the drawing board.

*Photo: Spencer Ackerman*
Info Dominance Vital to the 'Kill Chain,' Navy Intell Czar Says

Game-changing technologies will keep the service ahead of its rivals
(DEFENSE SYSTEMS 17 JUN 11) ... Henry Kenyon

The United States Navy may be the most powerful fleet in the world, but it must keep ahead of other nations seeking to claim regional and strategic superiority. A key strength of the sea service is information dominance, the ability to detect enemy forces, interfere with networks and act before the enemy. To meet the military challenges of the new century, the Navy has been developing new information dominance capabilities.

“Information dominance is required for every step in the kill chain,” Vice Adm. Kendall L. Card, director of Naval Intelligence and deputy chief of Naval Operations for Information Dominance. Speaking at a luncheon June 16, sponsored by the Northern Virginia chapter of the Armed Forces Communications and Electronics Association (AFCEA), he said that the U.S. must be able to disrupt the enemy’s kill chain and support systems.

Because the U.S. is the dominant military power on the planet, many other nations want to displace it, Card said. The U.S. must respond to these challenges with its own game-changing capabilities. But to meet these threats and to deploy new technologies, the Defense Department and the Navy must first get some things in order, he said. One issue is the DOD’s insatiable need for sensor data. Part of the challenge is to align and synchronize the capabilities of a variety of platforms to acquire and provide the information. While the DOD’s information transport capabilities are good, the government cannot keep up with the massive demand for data, Card said.

The Navy must optimize how it collects and manages data so that it can put its people in the right place to analyze it, he said. The Army deploys its information assets forward while the Air Force manages its systems from bases. The Navy, consisting of bases and ships, is a hybrid of these two approaches. In the future, the service must be able to get information to its ships, possibly in a satellite-denied environment, he said.

One area where the service has lagged behind and must now catch up is electronic warfare. The Navy is working on merging its electronic warfare capabilities with cyber operations. Card said this was necessary because the Navy is 19 years behind other nations when it comes to electronic warfare capabilities. The Navy and DOD being focused on fighting a war for a decade and the post-Cold War lull that preceded it caused the gap. He said that some nation’s electronic warfare suites are optimized to jam every radio frequency emitter in the Navy.

Recent efforts to catch up include programs like the Next-Generation Jammer and the Surface Electronic Warfare Improvement Program, said Card. Other areas of improvement include the activation of the 10th Fleet for Navy Cyber Operations. Despite looming budget cuts, he said that cyber capabilities are being fully funded and are a growth area in the Navy. Through the 10th Fleet, the service is improving its ability to increase network security and its exploitation
Info Dominance Vital to the 'Kill Chain,' Navy Intell Czar Says

and attach capabilities, he said.

The Navy is also building a family of intelligence, surveillance and reconnaissance systems to meet the service’s growing needs for more sensor data. One potential game-changing technology is the Navy’s carrier-launched unmanned combat aerial system (UCAS). Built by Northrop Grumman, the X-47 UCAS will determine how carriers are used for the next 30 years, he said. “It’s not about the capability, it’s about the future of manned and unmanned carrier systems,” Card said.

The Navy’s other unmanned aerial platform program is the Fire Scout robot helicopter. The program is doing well, and the service now has plans to evolve it into a medium-range sensor and weapons platform, he said.

The Navy is also addressing issues with how it tasks, collects, processes, exploits and disseminates collected sensor data. Card said that the Navy must make further use of the intelligence community’s data-sharing standards. The Navy does pull data from the intelligence services’ cloud into the Navy’s cloud. But the service needs to leverage this capability as much as possible, he said.

Ships and forward deployed forces must be able to access intelligence data from terminals such as the Distributed Common Ground System-Navy. Another challenge will be installing this capability on naval platforms to pull data from platforms such as maritime Global Hawks, he said.

Because a future major conflict could see a massive jamming of satellite communications, the Navy is looking at ways to operate without them. Card said that the Joint Aerial Layer Network is currently undergoing a test and review of a variety of alternative approaches to maintain connectivity.
ONR Announces Multimillion-Dollar 'STEM Grand Challenge'

(NAVY NEWS SERVICE 15 JUN 11) ... Office of Naval Research Corporate Communications

ALEXANDRIA, Va. -- Chief of Naval Research announced an incentive plan to award up to $8 million for ideas aimed at boosting K-12 education in the sciences, June 15.

Rear Adm. Nevin Carr made the announcement during the Naval STEM Forum, being held in Alexandria, Va., June 15-16.

"Today's approaches to training and education must seek new innovative ways to sustain America's position as a global technology leader," Carr told the more than 650 government, academia and business leaders gathered at the forum.

"I wouldn't begin to pretend that the Navy is going to solve the country's STEM problem… there are others out there working very hard to do that," Carr continued, "but we also want to make sure we are all intersected in a way that we can get the most out of the collective."

The challenge is one of many efforts the Navy has developed to encourage students, parents and teachers to pursue STEM education and careers. The Navy seeks to increase the talent pool of future Sailors, naval scientists and engineers through its STEM initiatives.

The Navy will award up to $1.5 million to each Phase One selectee. Teams will compete to advance to Phase Two. In the second stage, up to two teams will be awarded as much as $1 million each to extend their Phase One success to a Navy training challenge for another year. The technologies will be designed to meet students' individual learning style.

ONR will issue the proposal as part of its Long-Range Broad Agency Announcement for Navy and Marine Corps science and technology efforts. Contract awards are expected in fiscal 2012 and ONR officials anticipate multiple awards for Phase One.

In Phase One, participating Grand Challenge teams must develop an intelligent tutor, a system that uses computers and provides direct customized instruction to augment the classroom and serve as an aid for teaching middle to high school STEM curriculum. Teams will be evaluated on how well they demonstrate significant student improvement in retention, reasoning and problem solving, at an affordable cost. Based on these results, up to two teams will be selected to advance to Phase Two.

In Phase Two, selected team(s) must adapt their "tutor," or software, to effectively address Department of the Navy-specific training audiences and criteria. The winning team will be able to demonstrate a tutor that cost effectively produces significant improvements similar to its Phase One effort.
President Barack Obama is making a push to train 10,000 new American engineers a year, primarily with the help of the private sector.

Obama is trying to address the nation's persistently high unemployment level by boosting the number of people with skills in areas where unemployment is relatively low. Engineering fits that bill.

The unemployment rate in 2010 for all engineers was 4.5%. For software engineers it was 4.6%, and for all computing professionals, 5.4%, according to U.S. Labor Department data analyzed by the IEEE-USA.

"We've made incredible progress on education, helping students to finance their college educations, but we still don't have enough engineers," said Obama, who has compared the U.S. educational needs to those following the 1957 launch of Sputnik.

The U.S. had just over 1.9 million engineers in 2010, according to Labor Department data. Software engineers make up nearly half of that total. The number of employed engineers declined during the recession.

Obama, who outlined the goal on Monday, said the idea is to achieve the 10,000-engineer-increase without "a whole bunch of federal funding."
To boost engineering enrollments, Obama said private sector companies will promote science, technology, engineering and math education, offer students incentives to finish degrees, and help universities fund their programs. The participating companies intend to double their internship hiring.

What would an extra 10,000 engineering graduates accomplish?

In 2009, the U.S. produced 126,194 engineering graduates for bachelor's and master's degrees and for Ph.D.s.; increasing that total by 10,000 would add 8%.

If the White House focus is just on engineers with bachelor's degrees, that number totaled 75,320 in 2009; an additional 10,000 would boost the number of graduates by just over 13%.

In 2009, there were 41,967 master's degrees, and 8,907 Ph.D. degrees awarded, according to the IEEE-USA, which assembled this data from an American Association of Engineering Societies study.

"Engineers have always played a prominent role in driving innovation and creating jobs," IEEE-USA President Ron Jensen said. "We're pleased that our nation's leaders recognize this and look forward to working with the administration and Congress to strengthen America's high-tech workforce."

Obama outlined his goals Monday, outlining a push that he developed with the help of his Jobs and Competitiveness Council. That presidential commission has 26 members, including CEOs at several tech firms: Paul Otellini, the CEO of Intel; Ursula Burns, the CEO of Xerox; John Doerr, the venture capitalist at Kleiner Perkins Caufield & Byers; and Sheryl Sandberg, the chief operating officer at Facebook. The chairman of the Jobs and Competitiveness Council is Jeffrey
Obama: 'We Don't Have Enough Engineers'

Immelt, who is chairman and CEO of GE.

Obama said Otellini "is heading up our task force for the Jobs Council in helping to figure this out, because he understands Intel's survival depends on our ability to get a steady stream of engineers."

A report last year by the National Academy aimed at drawing attention to the U.S. production of science, engineering, technology and math talent, pointed out that the U.S. graduates more visual arts and performing arts majors than engineers. It also noted that the U.S. ranks 27th among developed nations in the proportion of college students receiving undergraduate degrees in science and engineering.
Navy Officers Fall Prey to the Thin Digital Line Between Personal & Professional Lives

The past week of news has highlighted an important question for our times: how much of a role should our personal life play in our work life? I argued last week that Anthony Weiner’s resigning was bad for America, mainly because his staying in office would have set a precedent that “naughty” things we do in our personal time need not derail our careers. This is increasingly important in the digital age when our personal lives are exposed to our colleagues in non-work contexts thanks to Facebook, Twitter, LinkedIn, and blogs galore — and thanks to companies like Social Intelligence that mine those sites for information about job applicants and perform ongoing social media monitoring of employees to confirm that they are complying with their employers’ social media policies.

Fellow Forbeser Paul Jankowski disagreed with me generally, but especially when it comes to public servants, arguing that their integrity is required in public and in private. That is the attitude the Navy has, and it’s taking a toll on their ranks of officers. The Washington Post reported last week that the Navy has fired a record number on commanding officers this year (Hat tip: my soon-to-be bureau chief in D.C., Janet Novack). The reason for the uptick? Social media:

Adm. Gary Roughead, the chief of naval operations, called the increase in firings “bothersome” but said the Navy was duty-bound to uphold strict behavioral standards, even when commanders are off-duty. He attributed the rise in part to the revolution in communications and technology, which has made it easier for sailors and their families
Navy Officers Fall Prey to the Thin Digital Line Between Personal & Professional Lives

to snoop on one another and then instantly spread the word — even from once-isolated ships at sea.

“The divide between our private and professional lives is essentially gone,” Roughead said in an interview. “People can engage in the debate — does it really matter what a commanding officer does in their personal life? We believe it does, because it gets right to the issue of integrity and personal conduct and trust and the ability to enforce standards.”

Sometimes what we do in our personal life is a factor for our professional performance, and sometimes it’s not. Do we all want to go the way of the Navy? How are we going to start drawing the line as more and more of our personal lives migrate online and thus into the vision of our employers and colleagues?

After a teacher in Nebraska slept with a 14-year-old freshman, her parents sued her school in 2009 claiming it should have looked at his MySpace page before hiring him and realized he was obsessed with sex. Should anyone who works with children who has sexual innuendos on his or her social networking page be screened out? Meanwhile, the new FTC-approved social media background check company, Social Intelligence, flagged a job applicant as “racist” for joining the Facebook group, “I shouldn’t have to press 1 for English. We are in the United States. Learn the language.” It flagged another as an illicit drug user, in part because of his or her support for the legalization of cannabis. Should our political views be incorporated into employment evaluations in this way?

Our personal lives are increasingly rubbing up against our professional ones. Either our professional tolerance for what people do in their off-hours will rise or our overly-
Navy Officers Fall Prey to the Thin Digital Line Between Personal & Professional Lives

examined lives are going to start to become repressed and boring ones.
Somali pirates are turning to increasingly sophisticated methods such as satellite phones, custom-made GPS systems, and even monitoring the Internet to hunt down targets.

Somali pirates aren't content just floating around in their fishing boats, looking for victims. These days, pirates off the Horn of Africa are turning to a sophisticated mix of weaponry, jerry-rigged GPS devices, and ingenious hacks of shipping-industry databases to hunt down prey. The resulting technology isn't just fascinating—it also has a real impact on foreign militaries who are fighting piracy.

In addition to random attacks on cargo and passenger ships, Somali pirates are increasingly relying on the use of GPS systems, satellite phones, and open-source intelligence such as shipping industry blogs in order to figure out the location of ships.

Much of the technological infrastructure used by the pirates is allegedly located in the Somalian city of Eyl, which has been described as the “piracy capital of the world.” In an interview with Abdullahi Jamaa of Egyptian web publication onislam.net, Andrew Mwangura of the East African Seafarers Assistance Program detailed the methods used by the pirates:

The most important thing for Somali pirates is getting relevant information regarding merchant vessels that they wish to hijack. But this does not come easily without the use
of certain technologies [...] What they must know includes information on the value of vessels, the value of the goods and the number of crew members [...] They use navigational technologies in their daily operation. This involves a combination of technologies, most important[ly] they use satellite cell phones for long range communications.

Satellite phones are easily attainable in the chaos of Mogadishu; foreign importers earn a hefty premium bringing the expensive phones into the beleaguered country. However, the most interesting weapon in the Somalian arsenal to western observers is the use of pirate-operated radar to locate targets at sea. Pirate “mother ships” with radar and advanced weapons capabilities have strayed far beyond the Horn of Africa to locales as far-flung as Madagascar, India, and the Persian Gulf.

According to the Christian Science Monitor's Ben Arnoldy, the “mother ships” use surprisingly modern tech, including radar and caches of equipment for breaking into fortified cargo ships.

Jamaa also notes that the pirates are turning to the use of open-source intelligence: They have translators who interpret the bulk of information that filters in through the automatic tracking devices. These men, though not involved in the actual hijacking, decipher and break down information for the team. The ‘foot soldiers’ are given instructions that most often turn out to be successful. The men who call themselves Somali Coast Guards also invest time on the World Wide Web tracking and gathering vital information. For example, the pirate financiers visit the Maritime Bureau Website to check what strategies have been put in place to curtail their activities. They, in turn, feed the gang.

According to the European Union, a sharp uprise in Somali pirate attacks is expected in 2011, including the use of machine guns as an everyday weapon. Western governments are, in turn, stepping up their game--Britain is taking steps to provide merchant ships with weapons, which would be the first time since World War II that this has happened.

[Image: Flickr user Rubygoes]
Somali Pirates Go High Tech
IPv4 to IPv6 Switch: When Protocols Collide

IPv4 to IPv6 switch: When protocols collide

By Lori MacVittie, 11 June 2011 09:00

COMMENT

Shifting from IPv4 to IPv6 will take years and could be a bumpy ride. But few organisations will find the process as complicated as cloud computing providers, says Lori MacVittie.

Not since the first packets were tossed around the internet has it faced so much potential change, with implications for its health and well-being and, peripherally, cloud computing.

The recent World IPv6 Day gave a host of vendors, providers and interested parties the chance to engage in a full-scale IPv6 interoperability test live on the internet. Yet for many of the participants it wasn't just a test of IPv6 compatibility but an examination of what is considered one of the most promising migration strategies: dual-stack support.

As its name suggests, the dual-stack option involves running IPv4 and IPv6 networking stacks on the same system as a means to communicate with other nodes regardless of which version might be used.

Advantages of the dual-stack option

It's considered the best of the options available — when compared with tunnels and translators — because it's the simplest of the options to implement and provides the widest coverage of endpoint combinations.

It's a strategy that allows for the reality that it's going to take a long time to migrate the entire world — every single device out there — from what has been the only standard the internet has really known to its successor, IPv6.

Given the reliance business, government and individuals have on the internet, there is no feasible way to accomplish a single, mass migration from IPv4 to IPv6. The process will be slow and take years. In the meantime, the onus is on those with a public-facing presence to somehow support both protocols.

Dual stacking meets that need well, because most infrastructure is already dual stacked. But running both stacks is not the same as using it to integrate and interconnect the myriad services — networking and application oriented — necessary to enable even the simplest of tasks to be completed.
DNS complexities

Consider the process of simply getting to a website, which is more complex than it sounds. DNS must be queried, packets routed, TCP sessions initiated, data exchanged. And that's only the tip of the iceberg.

“Given the reliance business, government and individuals have on the internet, there is no feasible way to accomplish a single, mass migration from IPv4 to IPv6.”

Inside the datacentre where that site resides is a multitude of components — hardware and software — that must interact to answer a query as simple as an ICMP echo request.

Being dual stacked does not necessarily address the need for services to support IPv6. Imagine an IPv4 endpoint requesting the IP address for a site. DNS must respond, but with what? Obviously an IPv4 address and not an IPv6 address.

Consider the reverse, as well. How does DNS know which IP version of the address to respond with? As we shift from one version to the next, we will be faced with...

...an environment in which both versions are active, and the infrastructure services responsible for making the internet go round must be able to support both, a more complicated task than it at first perhaps appears.

Few organisations will find the process of migrating from IPv4 to IPv6 as complicated as cloud-computing providers.

The impact on cloud computing

Cloud-computing providers, like everyone else, rely heavily on IP addresses to integrate and interconnect their vast array of compute, storage and network resources. But they are also responsible for providing public-facing services for their customers, such as DNS. Internally, they employ a complex ecosystem of scripts and management frameworks that enable the automation and remote control necessary for self-service.

So not only does a cloud provider need to ensure its external services are capable of supporting both versions, but they must migrate their internal systems, frameworks and controls.

For some cloud-computing providers, those supplying software-as-a-service (SaaS) in particular, this requirement is probably not as difficult as it will be for an infrastructure-as-a-service (IaaS) provider. That's because an IaaS provider must also deal with customers who configure and control
their own virtual images, many of which may be reliant on IPv4 instead of IPv6, or vice versa.

Applications and other services are often developed using IP addresses as identification of any external or third-party integrated services, and those applications are generally controlled by the customer, not the provider.

But that does not mean SaaS is off the hook. Applications deployed in any cloud-computing environment that integrate back into enterprise datacentres or vice versa, which may be using different IP versions but rely on IP addresses for security or integration, could be stymied by incompatibilities or incomplete migrations.

**Collaboration to avoid wide-scale outages**

There are myriad challenges to such a mass migration when so many different variables are involved, so it's not going to be a simple case of throwing a switch. The collaboration and careful planning that will be required to meet the challenges without causing wide-scale outages have just begun.

"As we've never attempted such a large transition before with the internet on its present scale, we must be prepared to cut everyone a bit of slack."

As we've never attempted such a large transition before with the internet on its present scale, we must be prepared to cut everyone a bit of slack. It is no trivial task that the internet as a whole is undertaking. If we understand the complexity of the task before us, we should be able to cope with the inevitable bumps in the road.

Perhaps considering how difficult a task cloud-computing providers — indeed all of us — have ahead, we'll be a little less condemning of outages and the like that occur from the collision of IPv4 with IPv6 during the months and years ahead.

*Lori MacVittie is responsible for application services education and evangelism at application delivery firm F5 Networks. Her role includes producing technical materials and participating in community-based forums and industry standards organisations. MacVittie has extensive programming experience as an application architect, as well as in network and systems development and administration.*
Welcome to a Faster Web

Monday, June 13, 2011

Welcome to a Faster Web
The first commercial deployment of SPDY, a protocol designed by Google to make websites faster, launches today.
By Erica Naone

SPDY, a protocol Google revealed in late 2009, dramatically speeds up Web page loading by changing the way that browsers communicate with servers. Until now, Google has only tested the research project internally and deployed it on a few of its own sites. But today, the protocol launches as a commercial product.

Website optimization company Strangeloop has built SPDY into its flagship product Site Optimizer, software that sits in between a website and its users, and adjusts the site's code to make pages load more quickly. Strangeloop's customers will have the ability to turn the protocol on easily; in tests, the protocol has sped up websites by 10 to 20 percent.

At first, this will only make a difference for people who visit websites using Google's Chrome browser (the only one that supports SDPY), but Strangeloop expects that it could end up having a big impact on mobile devices as well, since Google is likely to build SPDY into browsers designed for Android.

The speed with which a website responds to users is an increasingly important technical and economic issue. According to the content-delivery network Akamai, people only give a site three seconds, on average, to load before giving up and navigating away. Better performance often means more page views, and thus more interaction with users. For online shopping sites, this translates to higher sales.

It's not just individual sites that have an interest in speeding up the Web. Google has been working to make the Web as a whole faster, reasoning that the entire experience needs to be lightning-quick and smooth to keep people happily using its many services. Google also hopes to entice people to use more Web services and less desktop software (see, for example, its Chrome OS), and the company knows this won't be possible if they struggle with performance.

There are a lot of ways to speed up a website. Changing the protocols that determine how information gets sent over the Internet is potentially the most rewarding but also one of the trickiest. These protocols are fundamental to communication between websites and servers, so they can have far-reaching effects on website performance.
across all devices. However, to roll SPDY out to the entire world, all browser manufacturers would have to adopt it, and every server would have to support it, says Joshua Bixby, Strangeloop's president. This is a tall order, and so SPDY has "real implementation challenges," he says.

Strangeloop's existing product is, however, well-positioned to help Google make a start. Strangeloop already helps businesses speed up their websites by handling optimization for them without requiring them to change their code or hardware. The Site Optimizer software sits between a company's Web server and the user's browser and adjusts the website's code automatically to make it load faster; this already includes improvements customized for specific browsers. Site Optimizer customers can choose to turn SPDY on, making their servers behave as if the protocol were installed, for customers who visit their sites using Chrome.

Browsers today typically open up lots of connections to a server, in order to start downloading lots of information at once—images, ads, text, and so on. Tom Hughes-Croucher, chief evangelist for Joyent, a company that provides cloud software, explains that, while this does speed things up, the approach also has its problems. Those connections take time to "warm up" and start downloading at their full capacity. Also, they don't prioritize well, so the user might end up waiting for images at the bottom of a page to load when what he's really looking at is on top.

SPDY addresses this problem by opening one connection that is capable of loading many different parts of the page at once. It also allows programmers to manage how pages load, so they can deliver more important pieces first.

Strangeloop's product is designed to handle using SPDY, so customers don't have to worry about writing different code for users who do and don't use SPDY. The company worked extensively with Google engineers to get SPDY deployed and running effectively.

Bundling SPDY with existing optimization products is a good starting strategy for Google, says Eric Hansen, founder and CEO of the website optimization company SiteSpect. He expects Google to eventually include SPDY in its own optimization product, called mod_pagespeed, which is similar to Site Optimizer. Google needs to do whatever it can to get websites to adopt SPDY, he says, because that's the biggest part of its "uphill battle" to gain acceptance for the protocol.

Bixby believes that websites will become more willing to use SPDY when they see its potential benefits. "What's really exciting to me is its capabilities on the mobile side,"
Welcome to a Faster Web

Bixby says. Google hasn't yet built SPDY into Android's browser, but when it does, the protocol stands to make an even bigger difference. Since mobile Internet browsing is painfully slow and Android handsets have a large portion of smart phone market share, Bixby thinks SPDY could make a difference in that arena. He says, "I would be very surprised if we don't see this in Android in the near future."

Copyright Technology Review 2011.
Reassured by a relatively smooth test of IPv6 last week, some Web sites are choosing to keep servers available over the next-generation Internet technology.

And that’s good news for an Internet that's bursting at the seams. The results of the test, called World IPv6 Day, may help encourage others to make the IPv6 upgrades.

In the test, a number of organizations broadcast that their servers were available on IPv6. That meant anybody who had an IPv6 Internet connection would get that version of the server rather than the usual IPv4 one.

"There is a great sense of relief that nothing bad happened," said Alain Durand, director of software engineering at network equipment Juniper Networks and a former IPv6 leader at Comcast and Sun Microsystems. "It's a big sense now that IPv6 is a mature technology that is ready to be deployed."

Internet Protocol version 6 solves what has become a significant limitation of the present IPv4 technology: a dearth of new IP addresses that devices need to exchange information over the Internet.

A small fraction of people--well under a tenth of a percent by several estimates--have network configuration problems that broke access to IPv6 sites on the Internet. But the test went well enough that IPv6 is here to stay.

For example, Google decided to keep the main YouTube.com site available over IPv6. And Facebook concluded it will continue to offer the IPv6 version of its Facebook developer site. And according to data from RIPE, the European organization that doles out IP addresses, others leaving their IPv6 services on at least for the time being include Sprint, Mozilla, and BBN Technologies.

Comcast, one of the largest U.S. Internet service providers, also participated in the test. It's been ramping up its own trials of IPv6 for customers, too: this month it began testing IPv6-based e-mail services and expanded IPv6 trials to San Francisco, Chicago, Philadelphia, and Miramar, Fla.

And to help people fix problems they may encounter, Microsoft and Apple offered new help pages. Consumer network equipment maker D-Link also is offering IPv6 troubleshooting help.

All of this activity indicates progress in dealing with the chicken-and-egg problem that has been IPv6. Ironing out the wrinkles is one thing, but providing content such as YouTube videos over IPv6 will provide an incentive for those who operate the Internet’s networking equipment to start handling the IPv6 traffic properly and link up with each other.

"If all goes well...content can go to IPv6, and access can follow," said Lorenzo Colitti, Google's IPv6 guru, in a presentation about World IPv6 Day (PDF).
RIPE, which doles out Internet addresses in Europe, monitored IPv6 availability of various sites on the Internet during World IPv6 Day, and several sites are maintaining IPv6 availability even after the end of the June 8 test. The light green color on the chart shows 100 percent availability for IPv6 services; light blue shows no availability. The 24-hour test can be seen in the time block when more light green shows.

(Credit: screenshot by Stephen Shankland/CNET)

**Why all this hassle?**

IPv6 follows on from the present IPv4 technology, which provides only 4.3 billion IP addresses. That may sound like a lot of addresses, but it turns that people want to attach a lot of servers, PCs, phones, tablets, smart meters, automobiles, TVs, video game consoles, and home broadband network routers to the Internet. And until recently, moving to IPv6 was largely optional, so few bothered with IPv6's expense and difficulty.

Computer administrators could postpone IPv6 transitions because technology such as network address translation (NAT) let home broadband users, Internet service providers, and corporations share a single IPv4 address among multiple devices. There are drawbacks to NAT, but the approach lets people get more use out of IPv4. But the IPv4 address shortage has become much more acute: at the central domain of the Internet, the last IPv4 addresses were allocated in February, and now the shortage is propagating down through the IPv4 sales channels.

IPv6 is vastly more spacious. It offers 340 undecillion IP addresses—or 340,282,366,920,938,463,463,374,607,431,768,211,456 if you're being precise—by using 128-bit IP addresses rather than IPv4's 32-bit addresses. Assigning unique IP addresses means devices that are second-class Internet citizens because they're hidden away behind NAT networking layers become full peers on the Net. That could increase security worries, but it also opens up new frontiers such as easier peer-to-peer communications.
IPv6: Come On In, The Water's Fine

Arbor Networks' measurements of IPv6 traffic from six ISPs showed that it doubled during World IPv6 Day--the time period under the higher dotted line--but remained a tiny fraction of overall Internet traffic. However, IPv6 traffic ended up higher even after the end of the day.

(Credit: Arbor Networks)

In the distant future, everybody will have IPv6-capable computing devices that use an IPv6 Internet to get to IPv6 services. For now, though, it's a patchwork of IPv4 and IPv6 equipment.

To stitch things together, there are a number of approaches. "Dual-stack" equipment that can communicate with either version of IP is the eventual solution, but in the meantime, there are various approaches such as Teredo, 6RD, 6to4, 6in4, and DS-lite to bridge the gap. Teredo is good for individuals testing the waters, but 6RD has larger-scale abilities that have been proven at French ISP Free.fr and seems to be gaining clout.

"6RD is an important IPv6 transition technology, as is plays a key role at the beginning of and during the IPv6 migration, said Daisy Sun, a product manager at IP testing company Ixia.

The transition will take years.

"We cannot abandon IPv4 right now," Durand said. "This is going to stay for the next five years, ten years, fifteen years--maybe even more."
IPv6: Come On In, The Water's Fine

6rd Use-Case 1: From/to Internet

Bridging between IPv6 and IPv4 is complex. One approach, used by French ISP Free.fr, is called 6RD. With it, IPv6 data can be encapsulated within IPv4 data packets to traverse the existing Internet.
(Credit: Free.fr)

IPv6 test results
Getting to IPv6 hasn't been easy. It's been a standard for more than a decade. A number of organizations with a vital interest in it, though, organized IPv6 Day to help try to break the logjam. It began with major Web sites--Google, Yahoo, and Facebook--and content delivery networks Akamai and Limelight Networks. The first three house a huge amount of content people on the Net consume, and the latter two play an important role on the Net by helping to ensure data from a single Internet site is available globally. Organizing the day was the Internet Society, an advocacy and standards group. Participation ballooned to include more than 1,000 participants—a tiny fraction of the companies, schools, governments, individuals, and others on the Net, but a strong turnout nonetheless. To try to smooth out difficulties some people might have, many directed Internet users in advance to an IPv6 readiness test site.
So, for 24 hours on June 8, many turned on IPv6 services. Some had offered IPv6 services before, but only on an IPv6-specific domain such as ipv6.google.com. With test, google.com itself became available over IPv6.
"World IPv6 Day turned out to be everything we expected. For most of the end users of the Internet it was a non-event, which is what we were hoping for. At the same time it was a good learning experience," said John Curran, chief executive of ARIN--the American Registry for Internet Numbers that allocates IP addresses. He expects that will help encourage others to move to IPv6.

"A lot of the organizations that might have had concerns about turning on IPv6--they can now do that on their own schedule. It removes a bit of uncertainty they had about whether they'd be risking their business," Curran said. "If you look at top sites on the Internet, we're all turning on IPv6, and the Internet did just fine. We can deploy IPv6 in parallel in safety."

NTT America, which offers IPv6 services, had another important and reassuring data point for IT administrators: "The event did not result in an increase in customer support load," said Shawn Morris, manager of IP development.

The company pushed hard to make the test real. "We worked with both our customers and peers to turn up as much IPv6 connectivity as possible to make the day as successful as we could. IPv6 traffic volume on our network nearly doubled as a result of the event," Morris said.

Fundamentally, Curran thinks the positive results of the test could be a more effective incentive than the doom-and-gloom warnings that arrived a few months ago with the IPv4 exhaustion at the high level.

"It's going to have a very significant effect over the coming months," he said of World IPv6 Day. "I think this event potentially was more significant because it doesn't talk about a problem, it talks about a solution."
Arbor Networks' measurements showed a significant increase in content traffic being sent over IPv6 during the test. In particular, during business hours on the U.S. West coast, the blue HTTP traffic area indicating Web browsing activity--accounted for a large fraction of the IPv6 traffic.

(Credit: Arbor Networks)
Cyber Wargamers Set Sail Against Pirates

By Max Cacas, SIGNAL Connections
June 15, 2011

The Office of Naval Research is turning to a community of more than 1,000 cyber wargame players in a three-week effort to crowdsource new ideas on how to combat Somali pirates. The game carries the ungainly moniker of the Massive Multiplayer Online Wargame Leveraging the Internet (MMOWGLI) and aims at finding ways to defeat pirates operating off the northeast coast of Africa who have proved over the last several years to be a menace to commercial maritime shipping interests. Most recently, Somali pirates’ actions turned deadly in the Indian Ocean as they shot and killed four American hostages last February while the U.S. Navy conducted talks for their release.

Dr. Larry Schuette, director of innovation, ONR, explains that the game featuring Somali pirates as the enemy is part of “a pilot with our MMOWGLI to see if we can try to get people to come in with good ideas, in this case, on the piracy issue, and then team up and form up with other people online and get them to help solve our tough problems.”

Schuette says invited users, who will be drawn from academia, the defense community, government and nongovernment organizations, will play the game through a special secured website. “I would liken this to a sophisticated wiki, as opposed to a first-person shooter game. This is an online ‘card deck,’ where you essentially tweet your idea in the first round, 140-character ideas, so it’s less graphic and more text. The idea is to harness in the virtual world the ideaspace, if you will.”

He says MMOWGLI players will be evaluated two ways. One, moderators from the Naval Postgraduate School “will be online, looking at people’s ideas,” and deleting those that are irrelevant to the game. “If it’s a really good idea,” he continues, “and the moderator says ‘that’s really good,’ you can give it a thumbs up, if you will.”

Schuette says other players will be able to see each other’s ideas, “and as you do in a comments section of an online newspaper, you can say ‘I like that,’ ‘it’s a good idea’ or ‘it’s a bad idea.’”

He goes on to say that the crowdsourcing of ideas through the MMOWGLI is “critical here. It’s the online suggestion box, where the people who are suggesting have a vote on whether it’s a good or bad idea.”

Schuette says that the Palo Alto, California-based Institute for the Future designed the MMOWGLI. “When we were looking for a way to do an online game, all roads led back to them in this kind of game design.” The Naval Postgraduate School is the developers and programmers for the game, as well as the game directors, he adds.
RIM PlayBook Holds Security Edge Even As iPad Wows US Troops

RIM Playbook Holds Security Edge Even As Ipad Wows U.S. Troops
(BLOOMBERG NEWS 22 JUN 11) ... Traci McMillan and Melissa Aparicio

Research in Motion Ltd. (RIMM)’s PlayBook tablet computer, panned at its April debut, has an edge over Apple Inc. (AAPL)’s iPad in the Army thanks to RIM’s encrypted servers.

That advantage may soon dissipate as Apple’s more broadly popular devices march toward Defense Department security certification, which may come as early as this month, military officials said.

Tablet computers are being tested across all military branches, according to interviews conducted by Bloomberg Government since May 17. The services pay $500 to $600 per tablet, less than half the cost of laptops that are “ruggedized,” or enhanced with a shell and toughened to withstand harsh environments. Tablets also may replace paper manuals, maps, biometric devices and some communications tools.

The U.S. Army is leaning toward the PlayBook because RIM “addressed security concerns from the get-go,” said Lieutenant Colonel Matthew Dosmann, who oversees mobile device pilot-testing for the Army’s cybersecurity division. Security remains an issue for Apple and may hold back wider use of iPads, he said.

Apple, Dell Inc. (DELL), RIM and other tablet makers are vying to tap the military market for computers, laptops and servers worth $2.9 billion in the government’s 2010 fiscal year. Of that amount, spending on enhanced laptops was $33 million. The department spent $37 million on tablets in the same fiscal year, according to Bloomberg data.

‘Disruptive Technology’

Tablets are a “disruptive technology” that can replace heavier and more expensive equipment, Dosmann said. “As an infantry soldier, the last thing I want is something more to carry.”

To secure the devices so they can only be accessed using the common access card carried by all military service members and Defense employees, the services must install additional software or hardware, Gary Winkler, the Army’s former program executive officer for enterprise information systems, said in a June 20 telephone interview. Winkler oversaw about $4 billion, or 56 percent, of the Army’s information-technology budget.

“It’s very tough to drive the manufacturers to make the tablets and the devices with the embedded security that only the Defense Department needs or only parts of the federal government needs because the market just isn’t big enough,” said Winkler, who now heads Fairfax, Virginia-based Cyber Solutions and Services Inc., a government consulting and contracts support company.

Secure Servers

The iPhone and iPad already interact with the common access card, or CAC, and will be approved soon, possibly this month, Winkler said. Security engineering is under way for Google Inc. (GOOG)’s Android operating system. Microsoft Corp. (MSFT)’s Windows Mobile operating system was CAC-enabled more than a year ago.
BlackBerry smartphones, which run on RIM’s secure servers, already are approved by the Defense Department and in use on the battlefield. The PlayBook runs on the same servers, Dosmann said.

The Defense Contract Management Agency, which oversees defense contractors’ performance, is pilot-testing about 20 tablet computers, including the iPad and PlayBook, Jacob Haynes, acting chief information officer for DCMA, said in an interview.

“The next six months are going to be the biggest six months in mobile IT history, especially for the federal government,” Haynes said.

Security concerns haven’t reduced enthusiasm for iPads among military service members. Aircrews in the U.S. Marines, Air Force and Navy are using iPads unconnected to the Internet.

**Flight Bags**

The Air Force’s Air Mobility Command is testing iPads as a replacement for the traditional flight bag pilots use to store paper navigation charts and manuals. Travis Air Force Base in Fairfield, California released an invitation for bids for 100 black iPad 2s, according to a May 25 online notice.

“Tablet devices represent a totally new technology with flexibility and portability benefits that may reduce publication and printing costs across the command,” Kathleen Ferrero, a spokeswoman for Air Mobility Command, said in an e-mail on June 10.

The Navy has purchased 30 iPads to store aircrew documents, according to Amanda Greenberg, spokeswoman for the service. It’s also testing Android and Windows 7 operating systems, she said. BlackBerry is the only mobile device allowed to access Navy’s network at this point.

Dell, based in Round Rock, Texas, is testing its Streak tablet with Defense Department. “We are not trying to compete with the iPad,” John Marinho, Dell’s director of enterprise mobility and services, said in a telephone interview. “The iPad is a great device, but it’s a consumer device. It doesn’t address all of the pain points that we do.”

**‘Ruggedized’ Laptops**

Tablet procurements will spike before year’s end, Dosmann said, though some of the devices may not be allowed to access Army’s network.

Apple’s mobile operating system was the first tablet for which the Defense Information Systems Agency created a security procedure, said Lieutenant Colonel April Cunningham, a Defense Department spokeswoman. DISA is working on a procedure for Android devices.

IPads, PlayBooks and other tablets won’t completely displace the ruggedized laptops and other small computers in the department, Cunningham said.

“If you drop a couple $500 tablets and destroy them, then maybe you could have paid for a ruggedized laptop which may have better survived the impact,” she said.

**‘Ruggedized’ Tablets**
Companies are creating “ruggedized” tablets to solve this problem, said Frank Smith, CIO and vice president of Booz Allen Hamilton Holding Corp. (BAH), a strategic adviser for government agencies. Enhancing a tablet adds about 40 percent to its price, he said.

So far, the military services have bought tablets directly from manufacturers and through resellers in small lots. In the future, the Defense Department will use “traditional procurement methods” to buy the devices in bulk, Cunningham said.

Apple spokeswoman Trudy Miller and Research in Motion spokeswoman Jamie Ernst declined to comment.
The Web Is Shrinking. Now What?

JUNE 23, 2011 AT 11:30 AM PT

We all read the statistics every week documenting the meteoric new growth areas of the Internet, and they are impressive:

Online video is exploding, with annual user growth of more than 45 percent. Mobile-device time spent increased 28 percent last year — with average smartphone time spent doubling. And social networks are now used by 90 percent of U.S. Internet users — for an average of more than four hours a month.

None of this is a newsflash. Every venture capitalist, Web publisher, and digital marketer is hyper-aware of these three trends.

But what’s happening to the rest of the Web?

When you take these three growth areas out of the picture, the size of the hole left behind is staggering: the rest of the Web — the tried and true core that we thought would have limitless growth — is already shrinking.

Here are the facts:

When you exclude just Facebook from the rest of the Web, consumption in terms of minutes of use shrank by nearly nine percent between March 2010 and March 2011, according to data from comScore. And, even when you include Facebook usage, total non-mobile Internet consumption still dropped three percent over the same period.

We’ve known that social is growing lightning fast — notably, Facebook consumption,
The Web Is Shrinking. Now What?

which grew by 69 percent — but now it’s clear that Facebook is not growing in addition to the Web. Rather, it’s actually taking consumption away from the publishers who compete on the rest of the Web.

And just what is the rest of the Web?

I have been calling it the “document Web,” based on how Google and other Web architectures view its pages as documents, linked together. But increasingly, it might as well be called the “searchable Web” since it’s accessed predominantly as a reference, and navigated primarily via search.

And it’s becoming less relevant.

In the last year, Facebook’s share of users’ time online grew from one out of every 13 minutes of use nationwide, to one out of every eight. In aggregate, that means the document Web was down more than half a billion hours of use (that’s more than 800 lifetimes) this March versus last March. And in financial terms, that represents a lost opportunity of $2.2 billion in advertising inventory that didn’t exist this year.

The Creation of a New, Connected Web

The change in the Web’s direction is a clear indication to me that we aren’t just in the midst of a boom for new interaction modes, but rather in a generational overhaul of the Internet.

What replaces the declining searchable Web is a new and “fully connected” digital life. You may have heard this before. After all, the promise of the Web was to connect pages with hyperlinks. Well, this time, “connected” means much more. It means the Web connects us, as people, to each one of the individuals online; and those connections, ultimately, extend from one of us to all of us.
The Web Is Shrinking. Now What?

Just as significantly, this all happens in real time, and at nearly all times.

And here’s what’s different when you connect people, as opposed to pages: Now, the Web knows who we are (identity), is with us at all times wherever we go (mobile), threads our relationships with others (social), and delivers meaningful experiences beyond just text and graphics (video).

The connected, social Web is alive, moving, proactive, and personal, while the document Web is just an artifact — suited as a universal reference, but hardly a personal experience.

The Social Web Versus the Searchable Web

Analytical explanations — increasing smartphone penetration, bandwidth availability, and technology sophistication — fill in some of the gaps as we try to understand this sea change, but they fall short.

Something larger is afoot, and it’s not about science or technology. Rather, as human beings, we have changed how we fit the Internet into our lives.

And the nature of the Web is changing to match. The old searchable Web is crashing; while the new connected, social Web is lifting off.

The implications for publishers are massive.

The last decade has been defined by the rise of Google as the nearly limitless supplier of traffic to digital media properties. And so a generation of digital media publishers developed and followed the same playbook: create lots of content around top keywords, engineer for search engine optimization (SEO) and expand the surface area in search engines to reach more users. The objective was to catch visitors in their net; expand reach — as measured by ComScore — look more impressive to advertisers and capture
more demand.

The landscape is changing, and fast.

SEO’s strategic value is quickly fading as Google’s growth slows and its prominence in distribution slides away. In its place, Facebook has become the wiring hub of the connected Web — a new “home base” alternative to Google’s dominance of the last decade. Facebook began receiving as many visits as Google in March 2010, and already garners more than three times as many minutes as Google each month from users, according to comScore. Looking ahead, the best projections of U.S. online reach indicate that Facebook will surpass Google on that metric in less than a year, too.

And with this change, the nature of the relationship between users and publishers is being altered fundamentally — and perhaps forever.

Search offers a utility relationship, connecting users to content for the briefest of transactions; typically, it provokes users to just one pageview so they can find a piece of information, and then they move on.

But social discovery builds a relationship. Leveraging social endorsements and an environment of serendipitous discovery, consumers meet publishers in a meaningful context. As a result, the relationship that forms is stronger — and, more importantly for publishers, it’s branded.

Unlike the ecosystem set up by Google, where the search engine ironically intermediates between users and the objects of their queries (so that users reinforce their loyalty to Google, far more than to the publisher), in the world of social publishing, the Facebook hub enables a direct, if constrained, relationship between users and media brands.

The results — at least for my own company, Wetpaint — are that social media brings
The Web Is Shrinking. Now What?

more qualified eyeballs and retains them. People who come via social media stay longer on the first visit; and they are more likely to come back sooner and more frequently. Overall, our visitors from social networks have a relationship that’s several times stronger — and several times as valuable when measured in engagement, pageviews, and revenues — than the relationships people form when they arrive through search.

The Human Connection

But it’s not just a change in mechanics. It’s a change in our human relationships.

Lewis D’Vorkin, the Chief Product Officer at Forbes, speaks of it when he and Alex Knapp talk about “live” media, quantum entanglement and mutually rewarding relationships that bind authors and readers on the new connected Web. It’s a sense of the Web moving from static published reference to living digital companion.

But there’s even more, and this vast change foreshadows bigger and better impacts on our lives. The greatest innovators in social media are driving exactly along that edge today. As one friend commented recently on the full potential of connected lives, by being joined more closely together, we can increase empathy and meaning, while decreasing isolation.

Toward a Fully Connected Future

Admittedly, we’re early in the replacement cycle when it comes to the connected Web. Even for strong connected Web performers like Huffington Post, Wetpaint, and others, the sum total of traffic from Facebook, Twitter, video, and mobile may add up to only half the total, or less.

But the trend has tipped, and with that tip has come both the business necessity and the human impact potential of elevating the relationship.
The Web Is Shrinking. Now What?

As the document Web of old shrinks, the new connected Web expands and delivers experiences that make our time online more effective, efficient, and enjoyable.

And that changes the role of companies on the Web from mere content publishers or providers to truly connected digital partners for real people.

Ben Elowitz (@elowitz) is co-founder and CEO of web publisher Wetpaint, and author of the Digital Quarters blog about the future of digital media. Prior to Wetpaint, Elowitz co-founded Blue Nile (NILE). He is an angel investor in media and e-commerce companies.
Web Addresses Enter New Era

Web Addresses Enter New.Era

By SAM HOLMES And CHRISTOPHER RHoads

The dot-com era is over. Welcome to the dot-anything age.

On Monday, the organization that regulates the world's Internet domain names—yes, there is central coordination—approved changes that could allow anyone to register any name they like in almost any language as a Web address.

The new rules affect what the industry calls top-level domain names, the familiar dot-coms and dot-nets that end every Web address. Now, instead of having to use one of those existing forms, users will be able to end their addresses with the name of their company, such as dot-Ford, or their city, like dot-Berlin.

If successful, the change could alleviate a shortage of dot-com Web addresses and produce hundreds of millions of dollars in business for the companies whose business is managing the Internet's vast registries, as well as those selling the names, called registrars. Companies could gain new tools for highlighting their identities and networking with suppliers and distributors.

The shift, however, could also cause anxiety and disputes among governments, companies and other entities in safeguarding their brands and identities in cyberspace. Those seeking religious or political names, for example, could lead to sensitive situations.

For companies, even those that are happy with dot-com and aren't interested in adopting a new domain-name suffix will have to monitor the process to head off any potential trademark or brand-name infringement from other applicants, Internet experts said.
"Instead of having a dot-com that doesn't really mean anything, you will have an extension that means something," said Antony Van Couvering, the head of Minds + Machines LLC, a Santa Monica, Calif., company that advises clients on domain names.

The idea behind the change—which likely will need another 18 months before any of the new names become active—was to create more choice on the Internet and potentially spur innovation, according to the Internet Corporation for Assigned Names and Numbers, or Icann, the nonprofit Internet coordinating body that approved the measure.

For companies, having a Web-address suffix reflecting their own name could benefit branding as well as online security.

Online sales of counterfeit goods are on the rise, with fake domain names duping customers into thinking they are getting a good price on the real deal. Fraud is a problem, too.

To combat that activity, companies could register their brands as domain names—dot-brand—then offer authorized distributors of their products access to that domain, said Elisa Cooper, director of product marketing at MarkMonitor, a firm that helps businesses protect their brands online.

Those distributors would appear on the Web as distributor1.brand and distributor2.brand. Eventually, consumers could learn that only sites using
the dot-brand domain carry authentic products.

Shiv Singh, head of digital for PepsiCo Beverages-America, says the change creates interesting opportunities for building his brand. But he worries about the cost and wonders whether the new addresses will be adopted by consumers, noting that alternatives like dot-biz failed to find an audience. If it does catch on, companies like Pepsi may feel pressure to follow suit.

"I see this as nice to have, but it's not something we're going to get cracking on tomorrow morning," Mr. Singh said. "I am keen to see how other brands adopt it, because this will only succeed if it has critical mass adoption among companies."

Many companies opposed the change, however, citing the hassles it would create. Major companies typically register their name in multiple countries under country-code domain names such as dot-uk for Great Britain, as well as under multiple top-level domain names such as dot-com and dot-net.

The new rules create infinite options, compounding the registration issues. "Trademark owners and their lawyers are watching this closely to ensure their rights," said Jeff Brown, a spokesman for videogame publisher Electronic Arts Inc. "For us, the domains seem expensive and offer negligible value."
Web Addresses Enter New Era

Peter Dengate Thrush, standing, chairman of Internet Corp. for Assigned Names and Numbers, at an Icann meeting in Singapore on Monday with Rod Beckstrom, the organization's president and chief executive.

Search-engine giant Google Inc. warned that the change has the potential to create widespread user confusion.

"For example, if someone wants to find Citibank, would that be at citibank.com, www.citibank, citi.bank, or somewhere else?" a Google spokeswoman asked hypothetically.

Icann will accept applications for addresses under the new rules from Jan. 12 to April 12. The first of the new domains could be online by late 2012.

There are currently about 20 generic top-level domain names, like dot-org, and more than 200 country-code domain names, like dot-de for Germany. As of April, there were more than 211 million Web addresses in use around the world, with nearly half of those using the dot-com suffix, according to Matthew Zook, the head of ZookNIC Internet Intelligence, an Internet research firm.

Companies now will need to determine if they want to register their name under the plethora of potential new addresses. Ford Motor Co., for example, might eventually need to consider whether to register its name under a new dot-Texas suffix—ford.texas—to associate with customers there, or get a suffix using its own name, dot-ford.

"We need time to investigate but it sounds interesting," Said Deep, a spokesman for Ford, said Monday. "In the end, we will do what makes the most sense for our customers."

Since so many names are already taken on the popular dot-com suffix, the change could produce attractive alternatives like dot-web for entities that missed out.
Web Addresses Enter New Era

Not everyone will jump in, primarily because entry isn't cheap.

A company or government or individual that wants a domain-name suffix must pay Icann $185,000 just to apply. The application itself is several hundred pages long.

The fee could keep smaller businesses from registering a unique extension, even as the change opens up opportunities to build Web addresses on industry keywords like dot-pets, said Warren Adelman, president of domain-name registration firm GoDaddy.com.

Jason Levin, an online florist in Vista, Calif., who paid $2,500 on the secondary market for SunFlowerGuy.com, said he's unlikely to change his domain name under the new rules. "If we saw an opportunity that made sense, we'd consider it," Mr. Levin said. "But I'm not in the business of buying and selling domain-name extensions. I sell flowers."

For those who secure domain names, there is a yearly fee to Icann of around $25,000. That comes on top of the costs of running the domain-name suffix, likely outsourced to a company already in the business, which can run anywhere from $15,000 to millions of dollars, depending on the number of users, according to Ms. Cooper of MarkMonitor.

Icann said the hefty fee is based on the estimated cost of processing the applications, including possible litigation involving name disputes and other contingencies.

Applicants that look like cyber-squatters taking advantage of brand names or trademarks that clearly don't belong to them will be rejected, Icann said. An applicant seeking to register, for example, dot-cocacola, would have to be the well-known beverage company.

Winners otherwise will be determined by a panel that will consider factors like financial and technical capability, as well as how the applicant plans to
use the domain. Some contests for a single name could be resolved by an auction, potentially generating sizeable revenue for Icann.

Once an appealing domain-name suffix is secured, selling the secondary names—meaning the words to the left of the dot—could be a profitable business. Dot-doctor could be an attractive offering to the medical profession, said Adrian Kinderis, chief executive of Melbourne-based AusRegistry International, which sells names under country code domain names like dot-au for Australia and dot-om for Oman.

Dot-doctor, for example, could be made available to only licensed doctors, who would get Web addresses appearing as yourname.doctor.

"I could sell those for $1,000 a throw because you're adding value into the verification mechanism that exists," Mr. Kinderis said.

—Elizabeth Holmes, Stu Woo, Yukari Iwatani Kane, Shalini Ramachandran and Angus Loten contributed to this article.

Read more: http://online.wsj.com/article/SB10001424052702303936704576396963900727284.html#ixzz1QClBwzCF
Loosen the Cap on Employees' In-Boxes

Tight restrictions on e-mail size often just encourage people to work around the limits by sending files outside a company's control.

• FRIDAY, JUNE 24, 2011
• BY BRIAN BERGSTEIN

Companies can strengthen their computer networks against hacking attacks and data breaches, but their defenses won't work as well if employees are circumventing them. Yet companies often unintentionally inspire just such behavior by limiting how much e-mail their employees can send, receive, and store.

That's because employees who face tight limits on the size of their mailboxes tend to merely work around the restrictions. For instance, they might send and receive files through their personal Web mail accounts or through Web file-transfer sites. Using the public Internet could make it more likely for the information to be stolen, and there are consequences beyond hacking, too: once data leaves a company's control, it can be harder to restore it after a disaster or to find it during audits or lawsuits.

The employees at the Pump Solutions Group used to have strict limits on how much e-mail they could store because ballooning in-boxes required the company to buy, manage, and maintain more mail servers. But the pump manufacturer's global network manager, Jeff Rountree, has been lightening up on the policy and might get even more generous. He hired a company called Mimecast to handle the e-mail remotely — "in the cloud." That greatly reduced the need for Rountree to manage e-mail servers, which in turn could reduce the need for 700 of Rountree's coworkers to worry about the size of their in-boxes. Rountree likes that idea because if employees face no resistance to e-mailing large files, "in the long run, it's better for us to let them do it and we can monitor it," he says. "If we don't let them send it, we wouldn't know, because
Loosen the Cap on Employees' In-Boxes

they would find some other way to do it."

Mimecast is one of a growing number of options for companies that want to reduce the headaches of managing e-mail themselves. Many large companies use Google Apps, which also offers ways for companies to archive and otherwise maintain employees' e-mail. The cost of such cloud services is often a few dollars per employee per month. These services don't always remove mailbox caps entirely, but the limits are generous: Google's Gmail for business lets each employee have 25 gigabytes of mail.

Some Mimecast customers give their employees unlimited e-mail. Others, like Rountree, do set limits, because Mimecast routes messages through their local mail servers: Pump Solutions Group employees still get reminders to clear space by deleting old mail. But Rountree is exploring a significant increase in the limits, because Mimecast can reduce the load on the local mail servers by archiving old messages and "stubbing" other e-mails to reduce their file size. "Users wouldn't even have to worry about it," he says.
Fire Scout Proves Worth

Fire Scout proves worth
Published: June 16, 2011 at 7:07 AM

PATUXENT RIVER, Md., June 16 (UPI) -- The U.S. Navy says its Fire Scout unmanned helicopter is proving its ISR capability during its first land-based, Central Command deployment.

The Fire Scout, managed by Navy and Marine Corps Multi-Mission Tactical Unmanned Air Systems program office, deployed in late April to CENTCOM in response to a U.S. Department of Defense intelligence, surveillance and reconnaissance task force request.

The aircraft provides ISR services in northern Afghanistan.

"We are very pleased with Fire Scout's performance during both its ship-based and CENTCOM deployments," said Navy Capt. Tim Dunigan, the program manager. "The team has done an exceptional job testing and maintaining the system to ensure we could meet the warfighter's demands."

Fire Scout's initial flight in theater took place May 2, the U.S. Naval Air Systems Command said. Only 19 days later, PMA-266 Detachment Alpha established initial operational capability during its first tasked mission from the International Security Assistance Force's Regional Command North area of responsibility.

The Fire Scout system provides full motion video and imagery from its electro-optical and infrared sensor payload along with laser designation of targets for troops in the field.

With flight endurance of more than five hours, the system offers a long-dwell sensor with real-time, dynamic re-tasking capability to respond to tactical forces.
"Our team is very excited about the first expeditionary deployment of the Fire Scout system", said Navy Cmdr. Brian Stephens, officer in charge for PMA-266 Detachment Alpha. "In less than one month, we have flown more than 200 flight hours and completed more than 80 sorties and we are on track to fly 300 hours per month."

PMA-266 Detachment Alpha is a government-owned, contractor-operated deployment. The detachment includes a military OIC and assistant OIC, five Navy intelligence analysts and 21 Northrop Grumman contractors to conduct missions in support of RC North tasking.
To fly combat missions around the globe, the Defense Department’s Predator and Reaper unmanned aerial vehicles rely on satellite communication links that allow Air Force pilots to direct the aircraft from ground control stations based in the continental United States.

The communications-hungry drones consume large amounts of bandwidth to pipe battlefield video feeds and other sensor data back to intelligence centers and to forces on the ground. As a result, satellites are becoming overloaded by the never-ending demand. Experts say the problem will only grow worse as the services increase the number of remotely piloted aircraft in the skies.

The Defense Department’s space sector is struggling to keep pace with the proliferation of drones. Since the 2009 cancelation of the Air Force’s Transformational Satellite program, which was supposed to provide more capacity for overloaded military satellite communication networks, Air Force officials increasingly have turned to commercial providers to make up the difference. Nearly 80 percent of the U.S. government’s satellite communications capacity comes from the commercial sector, experts say.

Part of the challenge there for the Defense Department is providing a means for transmitting information securely over these networks. Communications routed through commercial providers are largely not protected to the same degree as transmissions over military-owned satellites, which require encryption and other security measures that safeguard them from attack. Though the ultimate plan is to move all of the Defense Department’s battle-hardened space-based communication needs onto military systems — a transition that analysts say could take years, even decades — Pentagon officials for the foreseeable future will remain dependent upon commercial providers to supplement the network.

“As satellites become more expensive and the government has less money, they are looking for ways to be able to increase the amount of satellite bandwidth available,” said William Ostrove, space systems analyst at Forecast International. “They don’t have money to buy their own so they’re going to commercial satellite operators ... to get that capacity without having to buy and launch their own satellites.”
Unmanned underwater vehicles (UUVs) represent some of the best operational investment opportunities for the U.S. Navy, and the service could use UUVs to offset submarine fleet reductions, says Adm. Gary Roughead, chief of naval operations.

“If we make the right decision on UUVs, we could perhaps absorb a smaller sub force structure,” Roughead said June 16 during an event sponsored by the Center for Strategic and International Studies.

UUVs would be cheaper to acquire and maintain than nuclear-powered submarines, which are among the most expensive vessels in the Navy fleet. UUVs would be ideal, he says, for “dull and dangerous” missions, remaining in one place with sensors saving and transmitting data. These have been the types of missions done by the Navy’s attack submarines.

Roughead framed his comments around a discussion about the pending clash in the 2020s between Navy shipbuilding plans and available funding. “We’re going to have the aging out of ships built in the 1980s,” Roughead notes.

At the same time, though, the Navy is going to have to embark on a program to replace its SSBN ballistic missile submarine force — a program that’s been estimated at $40 billion for procurement, with life cycle costs of more than twice that.

The Navy also has started to ramp up its purchases of Virginia-class attack submarines, and analysts have questioned how the service can afford both attack and missile subs in the coming years.

While trying to reconcile those needs and costs, Roughead says, the Navy also will have to do midlife overhauls on some Nimitz-class carriers while decommissioning others. Further, the service also is in the midst of starting its new carrier class, led by the CVN-78 Ford.

The Navy, Roughead says, is going to have to prioritize. “In the next year or two, we’re going to have to dig in and decide,” he says.

The service could find some of its answers with UUVs, which are the one area “where we stand to have the greatest operational breakthroughs,” he says.

Roughead says he’s more than just interested in UUVs. “I’m obsessed,” he says. The critical UUV attributes that the Navy needs to develop are sufficient procurement numbers, shipboard safety, endurance and power. UUVs have a “huge potential” to be “netted together” and sent into an area of interest, he says.

The service had hoped to leverage commercial UUV efforts — such as programs developed by oil companies — and tweak them for Navy use, but that equipment has failed to meet military requirements.
WRIGHT-PATTERSON AIR FORCE BASE, Ohio — Two miles from the cow pasture where the Wright Brothers learned to fly the first airplanes, military researchers are at work on another revolution in the air: shrinking unmanned drones, the kind that fire missiles into Pakistan and spy on insurgents in Afghanistan, to the size of insects and birds.

The base’s indoor flight lab is called the “microaviary,” and for good reason. The drones in development here are designed to replicate the flight mechanics of moths, hawks and other inhabitants of the natural world. “We’re looking at how you hide in plain sight,” said Greg Parker, an aerospace engineer, as he held up a prototype of a mechanical hawk
that in the future might carry out espionage or kill.

Half a world away in Afghanistan, Marines marvel at one of the new blimplike spy balloons that float from a tether 15,000 feet above one of the bloodiest outposts of the war, Sangin in Helmand Province. The balloon, called an aerostat, can transmit live video — from as far as 20 miles away — of insurgents planting homemade bombs. “It’s been a game-changer for me,” Capt. Nickoli Johnson said in Sangin this spring. “I want a bunch more put in.”

From blimps to bugs, an explosion in aerial drones is transforming the way America fights and thinks about its wars. Predator drones, the Cessna-sized workhorses that have dominated unmanned flight since the Sept. 11, 2001, attacks, are by now a brand name, known and feared around the world. But far less widely known are the sheer size, variety and audaciousness of a rapidly expanding drone universe, along with the dilemmas that come with it.

The Pentagon now has some 7,000 aerial drones, compared with fewer than 50 a decade ago. Within the next decade the Air Force anticipates a decrease in manned aircraft but expects its number of “multirole” aerial drones like the Reaper — the ones that spy as well as strike — to nearly quadruple, to 536. Already the Air Force is training more remote pilots, 350 this year alone, than fighter and bomber pilots combined.

“It’s a growth market,” said Ashton B. Carter, the Pentagon’s chief weapons buyer.

The Pentagon has asked Congress for nearly $5 billion for drones next year, and by 2030 envisions ever more stuff of science fiction: “spy flies” equipped with sensors and microcameras to detect enemies, nuclear weapons or victims in rubble. Peter W. Singer, a scholar at the Brookings Institution and the author of “Wired for War,” a book about
War Evolves With Drones, Some Tiny as Bugs

military robotics, calls them “bugs with bugs.”

In recent months drones have been more crucial than ever in fighting wars and terrorism. The Central Intelligence Agency spied on Osama bin Laden’s compound in Pakistan by video transmitted from a new bat-winged stealth drone, the RQ-170 Sentinel, otherwise known as the “Beast of Kandahar,” named after it was first spotted on a runway in Afghanistan. One of Pakistan’s most wanted militants, Ilyas Kashmiri, was reported dead this month in a C.I.A. drone strike, part of an aggressive drone campaign that administration officials say has helped paralyze Al Qaeda in the region — and has become a possible rationale for an accelerated withdrawal of American forces from Afghanistan. More than 1,900 insurgents in Pakistan’s tribal areas have been killed by American drones since 2006, according to the Web site www.longwarjournal.com.

In April the United States began using armed Predator drones against Col. Muammar el-Qaddafi’s forces in Libya. Last month a C.I.A.-armed Predator aimed a missile at Anwar al-Awlaki, the radical American-born cleric believed to be hiding in Yemen. The Predator missed, but American drones continue to patrol Yemen’s skies.

Large or small, drones raise questions about the growing disconnect between the American public and its wars. Military ethicists concede that drones can turn war into a video game, inflict civilian casualties and, with no Americans directly at risk, more easily draw the United States into conflicts. Drones have also created a crisis of information for analysts on the end of a daily video deluge. Not least, the Federal Aviation Administration has qualms about expanding their test flights at home, as the Pentagon would like. Last summer, fighter jets were almost scrambled after a rogue Fire Scout drone, the size of a small helicopter, wandered into Washington’s restricted airspace.

Within the military, no one disputes that drones save American lives. Many see them as
advanced versions of “stand-off weapons systems,” like tanks or bombs dropped from aircraft, that the United States has used for decades. “There’s a kind of nostalgia for the way wars used to be,” said Deane-Peter Baker, an ethics professor at the United States Naval Academy, referring to noble notions of knight-on-knight conflict. Drones are part of a post-heroic age, he said, and in his view it is not always a problem if they lower the threshold for war. “It is a bad thing if we didn’t have a just cause in the first place,” Mr. Baker said. “But if we did have a just cause, we should celebrate anything that allows us to pursue that just cause.”

To Mr. Singer of Brookings, the debate over drones is like debating the merits of computers in 1979: They are here to stay, and the boom has barely begun. “We are at the Wright Brothers Flier stage of this,” he said.

Mimicking Insect Flight

A tiny helicopter is buzzing menacingly as it prepares to lift off in the Wright-Patterson aviary, a warehouse-like room lined with 60 motion-capture cameras to track the little drone’s every move. The helicopter, a footlong hobbyists’ model, has been programmed by a computer to fly itself. Soon it is up in the air making purposeful figure eights.

“What it’s doing out here is nothing special,” said Dr. Parker, the aerospace engineer. The researchers are using the helicopter to test technology that would make it possible for a computer to fly, say, a drone that looks like a dragonfly. “To have a computer do it 100 percent of the time, and to do it with winds, and to do it when it doesn’t really know where the vehicle is, those are the kinds of technologies that we’re trying to develop,” Dr. Parker said.

The push right now is developing “flapping wing” technology, or recreating the physics of natural flight, but with a focus on insects rather than birds. Birds have complex
War Evolves With Drones, Some Tiny as Bugs

muscles that move their wings, making it difficult to copy their aerodynamics. Designing insects is hard, too, but their wing motions are simpler. “It’s a lot easier problem,” Dr. Parker said.

In February, researchers unveiled a hummingbird drone, built by the firm AeroVironment for the secretive Defense Advanced Research Projects Agency, which can fly at 11 miles per hour and perch on a windowsill. But it is still a prototype. One of the smallest drones in use on the battlefield is the three-foot-long Raven, which troops in Afghanistan toss by hand like a model airplane to peer over the next hill.

There are some 4,800 Ravens in operation in the Army, although plenty get lost. One American service member in Germany recalled how five soldiers and officers spent six hours tramping through a dark Bavarian forest — and then sent a helicopter — on a fruitless search for a Raven that failed to return home from a training exercise. The next month a Raven went AWOL again, this time because of a programming error that sent it south. “The initial call I got was that the Raven was going to Africa,” said the service member, who asked for anonymity because he was not authorized to discuss drone glitches.

In the midsize range: The Predator, the larger Reaper and the smaller Shadow, all flown by remote pilots using joysticks and computer screens, many from military bases in the United States. A Navy entry is the X-47B, a prototype designed to take off and land from aircraft carriers automatically and, when commanded, drop bombs. The X-47B had a maiden 29-minute flight over land in February. A larger drone is the Global Hawk, which is used for keeping an eye on North Korea’s nuclear weapons activities. In March, the Pentagon sent a Global Hawk over the stricken Fukushima Daiichi nuclear plant in Japan to assess the damage.
A Tsunami of Data

The future world of drones is here inside the Air Force headquarters at Joint Base Langley-Eustis, Va., where hundreds of flat-screen TVs hang from industrial metal skeletons in a cavernous room, a scene vaguely reminiscent of a rave club. In fact, this is one of the most sensitive installations for processing, exploiting and disseminating a tsunami of information from a global network of flying sensors.

The numbers are overwhelming: Since the Sept. 11 attacks, the hours the Air Force devotes to flying missions for intelligence, surveillance and reconnaissance have gone up 3,100 percent, most of that from increased operations of drones. Every day, the Air Force must process almost 1,500 hours of full-motion video and another 1,500 still images, much of it from Predators and Reapers on around-the-clock combat air patrols.

The pressures on humans will only increase as the military moves from the limited “soda straw” views of today’s sensors to new “Gorgon Stare” technology that can capture live video of an entire city — but that requires 2,000 analysts to process the data feeds from a single drone, compared with 19 analysts per drone today.

At Wright-Patterson, Maj. Michael L. Anderson, a doctoral student at the base’s advanced navigation technology center, is focused on another part of the future: building wings for a drone that might replicate the flight of the hawk moth, known for its hovering skills. “It’s impressive what they can do,” Major Anderson said, “compared to what our clumsy aircraft can do.”


The Changing Shapes of Air Power

Drones are playing an increasingly important role in the American military. Only 10 years ago, the Pentagon had about 50 drones; now there are 7,000 drones in its inventory, ranging in size from large blimps to tiny Hummingbirds. Here are 10 drones currently on the battlefield or on the drawing board.

**AEROSTAT**

- 200 ft. long
- 65 ft. across the hull

Aerostats are tethered fabric balloons filled with helium that float 15,000 feet in the air from a single cable. They can lift 1,200 pounds, including a camera that pans 360 degrees for constant real-time surveillance. They are used extensively on the Afghanistan-Pakistan border and above Kabul, where one of them is anchored at Bala Hissar, an ancient fortress. Their virtue is that they can stay aloft for months at a time, carrying a heavy load of intelligence equipment. Their shortcoming is that they cannot be moved rapidly for new assignments.

**GLOBAL HAWK**

- 44 ft. long
- 116 ft. wingspan
Sometimes described as a “flying albino whale,” the Global Hawk is the largest flying drone. Although linked to humans on the ground, Global Hawks fly mostly on their own, guided by GPS coordinates they download from satellites. They were deployed over Afghanistan in 2001, providing commanders with battlefield images. The Global Hawk flies higher than the Predator and can stay up longer — for almost two days.

**X-47B**
- 38 ft. long
- 62 ft. wingspan
The Navy’s prototype combat drone, and the first combat drone able to take off from an aircraft carrier and land on it. Its first test flight (29 minutes) was on Feb. 7, 2011.

**REAPER**
- 36 ft. long
- 66 ft. wingspan
The largest armed drone. Called a “hunter-killer” aircraft, the Reaper can detect humans and can fire Hellfire air-to-surface missiles. It will soon replace the better-known Predator.
War Evolves With Drones, Some Tiny as Bugs

**PREDATOR**
- 27 ft. long
- 55 ft. wingspan
The Predator is the Cessna-size workhorse that has dominated remotely piloted flight since the Sept. 11, 2001, attacks. The Pentagon has 169 Predators in its inventory.

**FIRE SCOUT**
- 24 ft. long
- 27.5 ft. rotor diameter
The Fire Scout is designed to take off and land vertically. Last summer the operators of a Fire Scout drone lost control of it in the airspace over Washington, D.C.

**SHADOW**
- 11.3 ft. long
- 14 ft. wingspan
The little sister to the Predator, the Shadow is launched by a catapult, rather than from a runway. The drone is used by Army and Marine forces in the field. The United States recently sold a number to Pakistan.

**RAVEN**
- 3 ft. long
- 4.5 ft. wingspan
The Raven, which weighs just five pounds, is launched into the air by tossing it like a
War Evolves With Drones, Some Tiny as Bugs

football. It is carried by ground units in the field that need quick awareness of what may be around a corner.

HUMMINGBIRD

| 4 in. long |
| 6.5 in wingspan |

The prototype remote-controlled Hummingbird has a tiny camera in its belly and weighs less than two-thirds of an ounce. Propelled only by its flapping wings, it can fly at speeds up to 11 miles per hour, hover and perch on a windowsill.

INSECT SWARMS

The drones of the future. Researchers say there could be swarms of dragonfly-size drones — or smaller — by 2030.
Russia May Target US Sats With Laser Jet

Look Out Above! Russia May Target U.S. Sats With Laser Jet

- By Noah Shachtman | June 13, 2011 | 4:34 pm | Categories: Lasers and Ray Guns • @dangerroom • 1

Back in the early 80s, Soviet engineers began outfitting an Ilyushin–76 jet with a laser cannon. Two models of the “Falcon–Echelon” planes were flown — presumably as counterweights to U.S. efforts to construct a fleet of missile-zapping jets. But when the Soviet Union collapsed, the Falcon–Echelon program perished, as well.

Or so it seemed at the time. Now, there’s mounting evidence that the Russian military has revived the Soviet-era laser project. And in this new incarnation, according to The Space Review, the ray gun is aimed up — toward American satellites.

In many ways, the Beriev A-60 is reminiscent of the Airborne Laser Test Bed, the U.S. military’s laser-equipped 747 jet. Both planes feature a bulbous nose and odd-looking bumps in the fuselage. The ALTB’s nose opens up to give the ray gun inside a free path to blast oncoming missiles.

The A-60’s nose doesn’t seem to have any openings, however. Instead, there’s a “large bulge on the upper back of the aircraft [that] is apparently a sliding port for a 1-megawatt laser turret,” space historian Dwayne A. Day writes for The Review. “The laser is clearly intended to fire up, at something above the plane, rather than to the sides or down, to engage ground targets or other aircraft.”

The emblem on the side of the plane gives a clue what the intended target might be, overhead. In it, a falcon zaps a spacecraft as it travels over the North Pole and towards Russia. Day identifies the spacecraft as the Hubble Space Telescope.

A statement given to the Interfax news agency last year provides further evidence. According to an unnamed official, the A-60 system is “designed to transmit laser
energy to remote sites in order to counter the infrared opto-electronic tools of the enemy." In other words, the laser is supposed to blind American spy satellites.

The notion isn’t as fanciful as it sounds. Back in 1984, the Soviets trained a laser on the Space Shuttle Challenger, which it believed to be an orbiting spy. The laser “caused malfunctions on the Space Shuttle and distress to the crew,” according to Jane’s Intelligence Review. More recently, in 2006, China fired ground-based lasers at American satellites, temporarily obscuring the vision of the eyes above the sky.

Pictures of the resuscitated Russian laser jet began surfacing in 2009. By the summer of 2010, Pravda was openly touting the development of a “military airborne laser system based on the Ilyushin-76 and designed to counter enemy intelligence means in different environments.” Russian boss-for-life Vladimir Putin began talking about equipping Israeli drones with “space and laser technology.”

It’s not clear how far along Russian ray gun tech really is. But, ironically, the A-60 program appears to be heating up as the U.S. Airborne Laser Test Bed is cooling down. A planned fleet of ray gun–equipped 747s has been winnowed down to a single plane, and that one plane is misfiring during its tests. So the Russians may want to be careful about following the Americans too closely on this project. After decades of development and billions of dollars spent, the U.S. flying laser still can’t shoot straight.
Iran said it launched a satellite into orbit on Wednesday that Western aerospace experts said could be used for limited military reconnaissance and also to monitor crops and track damage from earthquakes, flooding and other natural disasters.

It was the second time that an Iranian rocket had carried a satellite into orbit and took place more than two years after Iran joined the international space club by launching its first satellite.

Iran released few details about the satellite, which it calls Rasad-1, or Observation-1. Western experts said it weighed about 100 pounds — meaning that the light payload and the modest rocket carrying it bore little resemblance to an intercontinental missile and its heavy warhead.

Still, aerospace experts said the successful launching demonstrated Iranian engineers’ growing skill and contrasted with the repeated failures endured by North Korea in trying to place payloads into orbit.

“It’s a significant step forward for the Iranians,” said Charles P. Vick, an expert on Iranian rockets at GlobalSecurity.org, a private research group in Alexandria, Va.

Still, it did not come as a surprise to those who monitor Iran’s efforts. “Everybody’s been expecting this,” said Marcia S. Smith, founder of SpacePolicyOnline.com, a news blog in Arlington, Va.

Mr. Vick noted that the Iranians had announced that Rasad-1 would be lofted last
After Delay, Iranians Launch a Satellite

summer, but the mission then was delayed.

“It’s taken them far longer than they advertised,” Mr. Vick said in an interview.

The reason, he added, appeared to be managerial failures and “sanctions that have been having a significant impact on their getting foreign technology and hardware.”

He described the Iranian satellite as an experimental craft designed mainly for tracking the Earth’s resources from space. But the spacecraft, he said, “could also be used for low-resolution reconnaissance.”

Iranian news reports said that the Rasad-1 was built by the Malek-Ashtar University. Analysts in the American intelligence community view the university as having close ties to the Revolutionary Guard, the Islamic Republic’s main enforcers.

Iranian scientists have long hailed the benefits of Earth-observation satellites for tracking floods, fighting fires, gauging earthquake damage, finding evacuation routes and identifying high-risk areas.

In February, President Mahmoud Ahmadinejad announced plans to launch several Iranian-built satellites this year, including at least one for reconnaissance. He also repeated a claim that Tehran would send an Iranian astronaut into space by 2020.

Iran placed its first satellite into orbit in February 2009. The nation’s 5,000 rial banknote, the equivalent of 50 cents, bears the satellite’s image. The Iranians called it a rudimentary communications craft.

The announcement of the launching on Wednesday came on the country’s Arabic-language television channel, Al-Alam.
After Delay, Iranians Launch a Satellite

The channel said a rocket known as Safir, or messenger, fired the satellite into an orbit with a maximum height of 162 miles. “It is capable of photographing the Earth,” the report said of the satellite.

The channel said Rasad-1 would circle the Earth 15 times a day and should operate for two months. Iranian media reports have said the Safir rocket can carry a satellite weighing 110 pounds into elliptical orbits as high as 280 miles.

Western nations fear that Iran is trying to develop a missile capability under cover of its space program that could also threaten to deliver nuclear warheads.

Iran denies that it has any ambition to develop an atom bomb and asserts that both its space and nuclear programs are peaceful.

But it is openly developing a group of increasingly large rockets. In theory, the biggest might eventually be powerful enough to hurl not only satellites into space, but also warheads between continents.
Astrobotic, CMU Build Lunar Lander in X Prize Bid

JUNE 15, 2011 4:32 PM PDT
Astrobotic, CMU build lunar lander in X Prize bid
by Tim Hornyak

As part of a bid to claim the Google Lunar X Prize, Carnegie Mellon University and Astrobotic Technology have completed structural assembly work on a lunar lander designed to deliver a roving robot to the surface of the moon in 2014. Taking off from Cape Canaveral, the lander will ride on a SpaceX Falcon 9 rocket, which had a successful maiden flight last year, on its four-day journey to the moon.

(Credit: Carnegie Mellon University)
Astrobotic, CMU Build Lunar Lander in X Prize Bid

Red Rover will explore the Apollo 11 landing site. (Credit: Astrobotic)
The craft will attempt a pinpoint landing, which would be a significant achievement. After deploying, the solar-powered, four-wheeled Red Rover will beam HD video in 3D to Earth as it explores the moon's Sea of Tranquility.
The Astrobotic-CMU team wants to reach the Apollo 11 landing site, which hasn't been seen directly in 40 years (though NASA has imaged it), and film it in HD.
The $30 million Lunar X Prize is aimed at fostering the first private launch that sends a robot to the moon. It has to travel some 500 yards and send video, images, and data to Earth.
The 5-foot-tall, half-ton aluminum lander has solar panels that can provide 500 watts of power, rechargeable batteries, eight thrusters, and four fuel tanks carrying almost 2 tons of propellant.
It will be able to carry the 173-pound Red Rover, which is mostly covered with solar panels under its camera mast, as well as 242 pounds of commercial payload.
The lander is set to be tested for structural integrity at a Boeing facility in El Segundo, Calif. Check out some pics of the assembly here.
Below is a video showing what Red Rover might look like as it negotiates the lunar terrain during its two weeks on the moon. What will it find at Neil Armstrong and Buzz Aldrin's old hangout?
More often than not, the Iridium satellite phone system is remembered as one of the great telecom flameouts of the 1990s. It almost became a literal one: At one point following a 1999 bankruptcy, the 70 or more satellites that make up the system were scheduled to de-orbit and burn up in the atmosphere, in what would have been a fiery denouement of Iridium’s epic bankruptcy case.

That didn’t happen. In 2001, at what was very nearly the last minute, a group of private investors nabbed the assets of the old Motorola-backed concern for fractions of a penny on the dollar, and kept the satellite phone service running. The timing was right. The 9/11 terrorist attacks, which led to wars in Afghanistan and Iraq, ensured that the U.S. Department of Defense would remain the system’s biggest customer, and it still is today.
And though no one will tell me with any certainty, it’s even possible that Seal Team Six used an Iridium-based communication system when they slipped into Pakistan and killed Osama bin Laden. Just sayin’.

The big mistake of the original Iridium was that it aimed to be “the phone” that globe-hopping executives would carry with them everywhere. In what could only be described as a monumentally bad judgement call on the state of the wireless market, common cellphones started working pretty much anywhere a mainstream user might happen to be, obviating the need for a single wireless phone that worked anywhere in the world.

Take out the word “mainstream,” and the business case for Iridium was and is strong. It finished its March quarter with 447,000 subscribers around the world — a 25 percent increase over the previous year — of which more than 315,000 are voice customers. They’re people whose jobs take them to the remotest corners of the globe — oil platforms at sea, drilling rigs in the desert, mines in mountainous terrain, you get the idea — and for whom being without a working phone is simply not an option. As big as the conventional wireless phone networks are, they still cover less than 10 percent of the globe. Government voice users — about 37,000 at last count — are the heaviest users, averaging about $140 in revenue each month, while commercial voice users — 279,000 at last count — average about $47 a month.

But the fastest-growing bit of Iridium’s business is in data. If you have a piece of equipment or an asset whose status or movement you have to track, even in a remote desert, across the ocean or at the South Pole, the chances are pretty good you can put an Iridium modem on it and follow its status in short regular bursts of data. This “machine to machine” or M2M business is small but growing fast. As of the last quarter, the business had 122,000 customers — nearly double the number from the year-ago quarter
— and brought in $6.4 million, accounting for about 10 percent of sales.

And here’s where you find another key difference of the new Iridium versus the old. Rather than anticipate every kind of use for the Iridium network, the company provides both the satellite data service and a modem module that third-party companies build into scores of applications as varied as tracking trucks across Brazil to buoys in the ocean watching for tsunami waves. There are some 150 third-party outfits putting the Iridium network to use today.

In 2009, the company went public. (I wrote about it for Businessweek at the time.) It raised $200 million to help finance a new $1.8 billion constellation of 81 satellites (66 plus 15 spares, some of which will remain on the ground) that are due to start launching on SpaceX rockets in 2015. And unlike its money-losing predecessor, this Iridium is profitable, having finished 2010 with $22.7 million on sales of $349 million.

Last week I caught up with Iridium CEO Matt Desch while he was on a swing through New York. We talked about what’s next for the Iridium satellite system more than a decade after most people had written it off as a failure. Today it’s anything but.

**Matt, Iridium came public about two years ago, well ahead of all these other tech IPOs that have been going on in recent weeks. How’s business been since then?**

**Desch:** Our initial plan was to do a more traditional private-equity to IPO process, but the world cratered in that time. And so going public was still important. We needed financing to pay for our next-generation satellite system, so we went public and then probably thought we’d do some high-yield debt offerings. But frankly we took advantage of the troubles in the world economy, and against that backdrop, export credit agencies really wanted to support their governments. We had a competition going on to build our
Seven Questions for Iridium...

new satellite system between the U.S. and France. The winner turned out to be France. Their policy to support their industry was a little faster-moving and had more depth than what the U.S. was able to do at the time. The French banks gave us $1.8 billion in financing at less than five percent interest over five years. And then we closed other financing last summer. So now we have a fully financed plan to obtain all the cash we need to fund our operations and build our next fleet of satellites. We continued to grow at an average of 25 percent over the last five years. We even grew through the recession.

Who’s building the new satellites and when will you start launching them?

We’re about four years into a five-year program. Thales Alenia Space is the prime contractor building them, but its a $2.3 billion multinational contract. SpaceX will launch them starting in 2016. We’re Elon Musk’s largest commercial launch contract. He’s still working on the platform, but we don’t need him for four years, so that’s going to be perfect timing. Lockheed is on the team. Even though they competed to build the satellites, they’re still going to write some of the flight software. Boeing is on the team and ViaSat is on the team and there are others. All told it will be 81 satellites, of which 72 will be launched, 66 will be operating with six orbiting spares, and then nine more spares on the ground.

Your traditional satellite phone business accounts for how much of your revenue, versus data and other things?

Phones account for about 50 percent, but the data business is growing the fastest. Everyone thinks that our business is limited to just satellite phones that provide voice services, and they worry that that business is going to get more competitive. Inmarsat introduced a new phone last year, and Globalstar is going to come back. But I’ve been saying for the last few years that its more complex than that. We’re going to change the
Seven Questions for Iridium...

rules around the personal device environment. We’re moving away from satellite phones to enabling people to work on the move a lot better. This will include using your smartphone in ways that you can’t use your smartphone today. Using devices like iPads and other things. Our business is more about working with partners who enable unique solutions that put our service to work rather than the old ‘I have a phone, do you want to buy it?’ model.

And what about data?

It’s our fastest-growing business. A couple of big things have happened in the last few years. Our network has always had some distinct advantages — it has the lowest latency and covers the entire planet. We’ve come out with some devices that are both really cheap and really small, we have more than 200 partners, and at least 250 of them put our modems into things that they don’t even tell us about. It may be aviation or shipping or fishing.

Back to the data business: Part of it is what’s called machine-to-machine communications. What is that, and why is it a big opportunity for you?

It’s still in early days, but it has expanded dramatically. That industry started on the terrestrial side. Other companies would put a cellular modem in devices like the handheld pad the FedEx delivery guys use, or for tracking the truck or a shipping container, or a train or a bus. Those applications are great, but they only have so much room. They’re limited by the coverage of the cellular networks. If you want to track a truck as it moves across Brazil and not just when it’s close to major cities, we end up getting built into those products. Satellite still only accounts for about one percent of that business, but it’s growing really fast for us. We’re talking like 50 to 60 percent a quarter, so its really exploding. Once you track something on the ocean, or in the desert or in the
Seven Questions for Iridium...

sky, we’re the best option. People say, well, 99 percent of the populated areas are covered, but there’s a lot of reasons why you might want to track something when it’s not in that populated area. It’s really enabling things that weren’t possible before. We end up solving a lot of high-value problems that governments and companies are willing to pay a few extra dollars for. It used to be that these things cost hundreds of dollars for the airtime; now it’s in the tens of dollars, so the cost is no longer an issue.

**So government is your biggest customer? And I presume a lot of that is the military? Was Seal Team Six using Iridium when they killed bin Laden?**

(Laughs.) Sorry, I can’t say. But yes, government accounts for about 25 percent of our business, and growing rapidly. We do things like Blue Force tracking — that is tracking so the good guys can see where everyone is, all the vehicles and people. Special operations guys do tend to use our system, and I’ll tell you why. The military has their own systems and their own satellites that they can pre-position when they have enough time to get ready. But special forces tend to work anytime, anywhere and on short notice. When the Navy was called in to help in Japan after the earthquake, they didn’t have anything they could use beyond the immediate area of the ship, so they used our system. When they go into a new place, sometimes we’re the only thing that will work for them, and their own systems are too expensive to set up. So, yes, the Department of Defense is a big customer, but commercial customers are growing much faster. A lot of the companies that use our system are smaller, and you won’t hear about them because they supply niche products to specific industries. There’s one in Salt Lake City that builds a product that’s built into trucks that monitors the driver to see if he’s riding the brakes or going too fast. In Australia they use our system to track trains in real time. At chemical and oil companies we’re used in “man down” products, where if the systems
detects you as motionless for several minutes, you have to hit a button to say you’re okay, because if you don’t you’re probably lying flat on the ground because you’re incapacitated or injured, and someone will come and rescue you. The list gets so long that we don’t even know about them all.

**Will you build an add-on for my iPhone that will let me make a call from some remote place where Verizon or AT&T’s network doesn’t reach?**

We won’t, but one of our partners might. My view is that you shouldn’t make a satellite phone to compete with the iPhone, because it will never be as cool as the iPhone or Android phones. What you really need to do is let them talk to our network so you can make calls on it and send messages and pictures. It probably won’t be any good for watching Hulu videos, but you will certainly be able to communicate and send pictures back and forth.
New LightSquared Plan to Reduce GPS Interference Greeted With Skepticism at House Hearing

New LightSquared plan to reduce GPS interference greeted with skepticism at House hearing

BY BOB BREWIN 06/23/2011
LightSquared's latest proposal to keep its planned broadband wireless network from interfering with GPS signals met with skepticism at a congressional hearing Thursday.

After multiple tests showed the network, as originally planned, would disrupt all GPS applications, the startup floated a fix earlier this week that it said would keep its initial transmissions at a safe distance from GPS frequencies.

The Defense Department, which developed and operates GPS and relies on the technology for all its operations, considers LightSquared network signals to be equivalent to a GPS jammer, according to a committee briefing memo prepared for today's hearing of the House Transportation and Infrastructure Committee Subcommittee on Aviation.

LightSquared said tests so far have shown that the lower block of frequencies it plans to use in its nationwide network of 40,000 base stations is largely free of interference issues, with the exception of a limited number of high-precision GPS receivers. The GPS system operates in the 1559-1610 MHz band and LightSquared operates in the nearby 1526-1536 MHz and 1545.2-1555.2 MHz bands.

The company said it will limit its initial operations to the 1526-1536 MHz band, which is "located farther away from the GPS frequencies, greatly reducing the risk for interference."

An aviation advisory group, the Radio Technical Commission for Aeronautics, told the Federal Aviation Administration on May 26 that in tests it had determined operations of LightSquared's transmitter in the lower band are "compatible with aviation GPS operations." But Margaret Jenny, president of RTCA, told the hearing that her group looked only at LightSquared transmitter broadcasts with a power of 1.6 kilowatts instead of the 16 kilowatts authorized by the Federal Communications Commission. She warned that higher power levels would render the results "far worse."

Jeff Carlisle, executive vice president for regulatory affairs at LightSquared, assured the panel the company would operate only at 1.6 kilowatts and not the higher power levels authorized by FCC, adding cellular equipment manufacturers do not even offer 16-kilowatt transmitters.

LightSquared eventually would like to operate in its upper frequency band, but Carlisle told the hearing that the company has no intention of compromising the safety of aviation or maritime
navigation systems, both heavily dependent on GPS. He vowed LightSquared will work with the GPS industry to resolve interference issues with GPS receivers, including development of filters to mitigate interference.

Phil Straub, vice president of aviation engineering for receiver manufacturer Garmin International, said such filters do not exist, and Thomas Hendricks, senior vice president of safety, security and operations at the Air Transport Association, said it would take a decade to develop them, hobbling full rollout of the Federal Aviation Administration's GPS-based Next-Generation Air Transportation System, which has a $20 billion price tag.

When FCC granted LightSquared a waiver to start operation this January, it directed the company to conduct interference tests and deliver a report by June 15. LightSquared requested and was granted an extension until July 1.

Roy Kienitz, undersecretary for policy at the Transportation Department, said the proposal LightSquared unveiled this week will require another round of tests on the lower band frequencies and their potential impact on GPS.

Craig Fuller, president of the Aircraft Owners and Pilots Association, a trade group that represents private pilots and corporations that operate their own aircraft, blamed FCC for the interference problems detailed at the hearing. He urged the committee to direct FCC to get a "sign off" from Defense and Transportation before allowing LightSquared to proceed with its network deployment.

Carlisle emphasized the high financial stakes LightSquared has in development of its network, with a $14 billion investment planned over the next eight years, projected to create 15,000 jobs a year in each of the five years it will take to build it.

Kienitz said airlines also have high stakes and cannot afford any interference with their signals. "GPS has to work 100 percent of the time when you are landing airplanes," Kientz said.

Rep. Thomas Petri, R-Wis., charman of the subcommittee agreed, and said, "there is no room for error" in aviation.
A Preview of Future Disk Drives

Monday, June 13, 2011

A Preview of Future Disk Drives
A prototype disk drive based on phase-change memory can outperform an off-the-shelf flash hard disk.
By Tom Simonite

A new type of data storage technology, called phase-change memory, has proven capable of writing some types of data faster than conventional flash based storage. The tests used a hard drive based on prototype phase-change memory chips.

Disks based on solid-state, flash memory chips are increasingly used in computers and servers because they perform faster than conventional magnetic hard drives. The performance of the experimental phase-change disk drive, created by researchers at University of California San Diego, suggests that it won't be long before that technology is able to give computing devices another speed boost.

The prototype created by the researchers is the first to publically benchmark the performance of a phase-change memory chips working in a disk drive. Several semiconductor companies are working on phase-change chips, but they have not released information about storage devices built with them.

"Phase-change chips are not quite ready for prime time, but if the technology continues to develop, this is what [solid state drives] will look like in the next few years," says Steve Swanson, who built the prototype, known as Onyx, with colleagues. It had a data capacity of eight gigabytes and went head-to-head with what Swanson calls a "high-end" 80 GB flash drive made for use in servers.

When it came to writing small chunks of data on the order of kilobytes in size, Onyx was between 70 percent and 120 percent faster than the commercial drive. At the same time, the prototype placed significantly less computational load on the processor of the computer using it. It was also much faster at reading data than the flash drive when accessing blocks of data of any size. The kind of large volume, small read and write patterns that Onyx excelled at are a hallmark of the type of calculations involved in analyzing social networks like those of Twitter, says Swanson. However, Onyx was much slower at writing larger chunks of data than its commercially established competitor.

Onyx was built using prototype phase-change chips made by Micron, a company working to commercialize the technology. The chips store data in a a type of glass,
using small bursts of heat to switch sections of the material between two different states, or phases, that represent digital 1s and 0s. In one phase, the atoms of the glass are arranged in an ordered crystal lattice, in the other they have an amorphous, disorganized arrangement.

Onyx's performance springs from the much simpler process of writing data to a phase-change chip compared to a flash chip, which stores data as islands of electric charge on chunks of semiconductor, says Swanson. Flash chips cannot rewrite single bits of information—1s or 0s—on demand. Instead they have to erase data in "pages" of a fixed size and then go back to program in the desired data. That limits the technology's speed. "It requires a flash memory device to have software keep a little log as it goes along of which data is correct," says Swanson. "With phase-change memory you can just arbitrarily rewrite what you need."

Sudança Gurumurthi, who researches computer architecture at Virginia Tech, says the San Diego project is a valuable demonstration of the true capabilities of phase-change memory chips. "Much research has simulated how they would perform, but this gives insights into complexities a simulation can't capture," he says. But it will be the price of the technology that will determine when it becomes a competitive technology, says Gurumurthi.

Gurumurthi's research suggests that using phase-change memory in combination with flash memory could see the new technology reach the market earlier than the day it is cheap enough to be used in dedicated drives. Simulations showed that adding a small buffer of phase-change memory to a flash-based drive could simplify the process of writing small chunks of data, the kind of operation where flash performs least well. "We found it significantly improves performance," says Gurumurthi. "That might be enough to offset the cost of adding a small amount of phase-change memory."

Copyright Technology Review 2011.
The 10 strangest facts about graphene

*By Lucy Sherriff, ZDNet UK, 10 June, 2011 13:56*

**ANALYSIS**

When first discovered, graphene was odd. Now odd is too small a word for a material seemingly set on winning all the records a material can win.

In the first part of our series, we looked at what graphene is and how it was discovered. In part two, we explored the different techniques we can use to make graphene.

But what is it that makes this material so remarkable? Here are 10 of the strangest facts about graphene.

**1. Strength**

"The most amazing thing to me about graphene is its strength. This is a sheet of atoms that you can pick up. That blows my mind."

So says Professor James (Jim) Tour of Rice University in Texas, and who are we to argue with that? A sheet of atoms that you can pick up: say it out loud to yourself a couple of times.

Everyone you ask about graphene's amazing properties says the same thing: it is really hard to pick one feature when the material is so astonishing. So let's consider a few more of them.

**2. No band gap**
Graphene has no band gap. A band gap is the gap between the energy of an electron when it is bound to an atom, and the so-called conduction band, where it is free to move around. An electron can't have an energy level between those two states.

This makes graphene a wonderful candidate for use in photovoltaic (PV) cells, for instance, because it can absorb photons with energy at every frequency — photons of different frequencies of light are converted to electrons with matching energy levels. A material with a band gap can't convert wavelengths of light that correspond to the forbidden energy states of the electrons. No band gap means everything is accepted.

This opens the tantalising possibility of highly efficient PV cells, but it's a problem if you want to use graphene in transistors, where you need the band gap to provide the isolation necessary if you want it to act as a switch that can be turned off.

It is possible to induce a small band gap in graphene by doping it. This is good enough for very fast amplifiers for radio work, but for transistors that make efficient logic circuitry you need a bigger gap.

3. Ballistic conduction

Yes, this is a really weird one: ambient temperature "unimpeded" conduction of electrons. It was observed in multi-walled carbon nanotubes at least as far back as 2002, and since graphene is basically an unzipped carbon nanotube, it does it too.

“The most amazing thing to me about graphene is its strength. This is a sheet of atoms that you can pick up. That blows my mind.”
The 10 Strangest Facts About Graphene

– Professor Jim Tour

The hexagonal lattice has the longest "mean free path" of any known material — of the order of microns. This is the distance an electron can travel freely without bumping into anything, or having its path disrupted by scattering; the things that induce resistance. When the mean free path is longer than the dimensions of the material, you get ballistic transport.

In graphene, the mean free path is of the order of 65 microns — long enough that electronic components could be made that would operate at ambient temperatures with virtually no resistance. This is similar to superconductivity, but at room temperature.

4, 5 & 6. Best at electricity

And in case that doesn't impress you, Manchester University's Dr Leonid Ponomarenko points out that graphene also has "the highest current density (a million times that of copper) at room temperature; the highest intrinsic mobility (100 times more than in silicon); and conducts electricity in the limit of no electrons". Which means it can carry more electricity more efficiency, faster and with more precision than any other material.

7. Transparency

Back to Professor Tour for this one: "Another amazing thing about graphene is that you can see it. You can lay a sheet on a white piece of paper and actually see it. It is amazingly transparent, absorbing just 2.3 percent of light that lands on it, but if you have a blank sheet to compare it to, you can see that it is there." That means you can see a single layer of atoms with your naked eye, if they're graphene.

As well as making graphene even more useful as a potential solar cell component, its transparency makes it ideal for use in touchscreens. Currently
The 10 Strangest Facts About Graphene

most screens are made from Indium Tin Oxide (ITO), which absorbs 10 percent of incident light. But ITO is quite brittle, whereas graphene is extremely...

8 & 9. Elastic
Well, for a crystal, anyway. Graphene stretches up to 20 percent of its length. And yet it is also the stiffest known material — even stiffer than diamond.

10. Thermal conductivity
Graphene also beats diamond in thermal conductivity. In fact, graphene now holds the record for conducting heat — it's better than any other known material.

11. Impermeable
Here's one for luck. Graphene is also the most impermeable material ever discovered. "Even helium atoms cannot squeeze through," Dr Ponomarenko says. This makes it a great material for building highly sensitive gas detectors, for example, since even the smallest quantity of a gas will get caught in its lattice, changing its electrical properties.

All of the above makes graphene a good contender for yet another record: the material with the most records. For a substance that's only been closely studied since 2004, this makes it the child prodigy of material science, and one well worth the intense interest it continues to generate.
Japanese ‘K’ Computer Is Ranked Most Powerful
By VERNE G. KOPYTOFF
Published: June 19, 2011

SAN FRANCISCO — In the rankings of the world’s most powerful supercomputers, a Japanese machine has earned the top spot with a performance that essentially laps the competition.

The computer, known as “K Computer,” is three times faster than a Chinese rival that previously held the top position, said Jack Dongarra, a professor of electrical engineering and computer science at the University of Tennessee at Knoxville who keeps the official rankings of computer performance.

K, built by Fujitsu and located at the Riken Advanced Institute for Computational Science in Kobe, Japan, represents a giant leap forward in speed. It will also undoubtedly be a source of national pride for Japan, at least among computer scientists, who take the race for fastest computer quite seriously.

“It’s a very impressive machine,” Mr. Dongarra said. “It’s a lot more powerful than the other computers.”

The latest ranking of the top 500 computers, to be released Monday, is determined by running a standard mathematical equation. The winning computer was able to make 8.2 quadrillion calculations per second, or in more technical terms, 8.2 petaflops.

The performance of K is equivalent to linking around one million desktop computers, Mr. Dongarra said.

Supercomputers are used for earthquake simulations, climate modeling, nuclear research and weapons development and testing, among other things. Businesses also use
the machines for oil exploration and rapid stock trading.

Building supercomputers is costly and involves connecting thousands of small computers in a data center. K is made up of 672 cabinets filled with system boards. Although considered energy-efficient, it still uses enough electricity to power nearly 10,000 homes at a cost of around $10 million annually, Mr. Dongarra said.

The research lab that houses K plans to increase the computer’s size to 800 cabinets. That will raise its speed, which already exceeds that of its five closest competitors combined, Mr. Dongarra said.

“K” is short to the Japanese word “Kei,” which means 10 quadrillion, the ultimate goal for the number of calculations the computer can perform per second.

K succeeded in pushing the previous leader, China’s Tianhe-1A supercomputer, at the National Supercomputing Center in Tianjin, China, to second place. Tianhe-1A had been the first Chinese computer to be ranked on top, signaling the country’s growing technological might.

The fastest computer in the United States, at Oak Ridge National Laboratory, in Oak Ridge, Tenn., placed third.

Asian countries have made huge investments in supercomputing and now dominate the upper echelon of the field. Japan and China hold four of the top five spots in the latest ranking.

However, in terms of the top 10, the United States remains the leader with five computers. They are at government research facilities.

Japan’s top supercomputer ranking is its first since 2004. The United States and China
Japanese 'K' Computer Is Ranked Most Powerful

are the only other countries to have held the title.

The rankings, which are issued every six months, change frequently and reflect how fast computer power is advancing. For example, the top ranked computer in June 2008, at Los Alamos National Laboratory in New Mexico, is now in 10th place.

Mr. Dongarra said a computer called Blue Waters, being developed at the University of Illinois at Urbana-Champaign, may rival K in speed.
Blowing up rockets in midflight is easy — as long as you’ve got a fast enough computer.

That’s the thinking at Artis, the Virginia firm trying to outfit the Army’s armored vehicles with so-called “active protection” technology — defenses that can stop incoming projectiles before they ever have a chance to hit. If the approach works, it could not only protect U.S. forces from rockets and missiles. It could shield troops from the most lethal roadside bombs, as well.

Rocket-propelled grenades and anti-tank missiles are some of the most potent weapons in the guerrilla arsenal, because they can punch through even the thickest armor. The Israelis, for instance, saw 40 of their tanks get hit by the projectiles in their 2006 war in Lebanon. So U.S. and Israeli defense contractors have tried all sorts of ways to blast these munitions while they’re still hurtling toward their target — to hit one speeding bullet with another, essentially.

But pulling off that trick shot requires a whole bunch of split-second calculations: from detecting the incoming rocket to figuring out its flight pattern to deciding when to fire the countermeasure. To do it all, you need a whole heap of processing power.

“Active protection is a testament to how fast computers are these days — especially when you’re not burdening them, by running an operating system,” says Artis CEO Keith Brendley.

Artis’ approach is a little more algorithm-intensive than others. Rather than blast the projectile early in its flight, Artis’ Iron Curtain system waits to fire its countermeasure until the very, very last moment, when the munition is just a few inches away from ramming into its target. Iron Curtain doesn’t shoot out at the projectile. Mounted on the
vehicle’s roof, it shoots *straight down*.

The idea is to minimize the harm to any civilians nearby — and to get as good a look at the incoming munition as possible before firing. But waiting does have a drawback; it means those life-or-death, bullet-on-bullet calculations have to be made even quicker that they would ordinarily.

“The further away from the vehicle, the harder the problem becomes,” Brendley, a former computer modeler at the Rand Corporation, tells Wired.com. “Which would you bet on: the physics becoming easier or the computers getting faster?”

Iron Curtain has pulled off the feat dozens of times in military trials, and is now undergoing safety reviews and component-level testing by the Army’s program manager for blast-resistant vehicles. Once that $5 million testing period is done — likely by the end of the year — it’s on to limited user tests, where the Iron Curtain will be mounted on the armored, off-road vehicles currently used in Afghanistan. The system won’t be heading to the war zone immediately, despite what you may have read in previous reports. But by this time next year, limited production of Iron Curtain could be underway.

Brendley, meanwhile, is looking for even tougher targets to knock down. Rocket-propelled grenades fly at 295 meters per second — pretty damn fast. But Iron Curtain’s smacked away these weapons so consistently, Brendley started looking at even quicker threats: namely, the explosively formed projectiles that were, for a time, the deadliest weapon of the Iraq insurgency. These “superbombs” fire out armor-piercing jets of molten metal at a blinding two to four kilometers per second — 10 times as fast as the grenades.

Darpa — which originally backed Iron Curtain — provided a bit of cash for Artis to build a “brassboard” pre-prototype for this superbomb-smashing system. In tests held over
the Christmas week, the Artis system held its own.

“Even I was surprised,” Brendely says. “Let’s face it: it’s kind of hard to believe you can intercept something that fast.”
When the Problem Is the Problem
Finding the right problem is half the solution
By ROBERT W. LUCKY / JULY 2011

Illustration: Greg Mably
A problem well stated is a problem half solved.
—Inventor Charles Franklin Kettering (1876–1958)

We're all fairly good at problem solving. That's the skill we were taught and endlessly drilled on at school. Once we have a problem, we know how to turn the crank and get a solution. Ah, but finding a problem—there's the rub.

Everyone knows that finding a good problem is the key to research, yet no one teaches us how to do that. Engineering education is based on the presumption that there exists a predefined problem worthy of a solution. If only it were so!

After many years of managing research, I'm still not sure how to find good problems. Often I discovered that good problems were obvious only in retrospect, and even then I was sometimes proved wrong years later. Nonetheless, I did observe that there were some people who regularly found good problems, while others never seemed to be working along fruitful paths. So there must be something to be said about ways to go
When the Problem Is the Problem

about this.

Internet pioneer Craig Partridge recently sent around a list of open research problems in communications and networking, as well as a set of criteria for what constitutes a good problem. He offers some sensible guidelines for choosing research problems, such as having a reasonable expectation of results, believing that someone will care about your results and that others will be able to build upon them, and ensuring that the problem is indeed open and underexplored.

All of this is easier said than done, however. Given any prospective problem, a search may reveal a plethora of previous work, but much of it will be hard to retrieve. On the other hand, if there is little or no previous work, maybe there’s a reason no one is interested in this problem. You need something in between. Moreover, even in defining the problem you need to see a way in, the germ of some solution, and a possible escape path to a lesser result, like the runaway truck ramps on steep downhill highways.

Timing is critical. If a good problem area is opened up, everyone rushes in, and soon there are diminishing returns. On unimportant problems, this same herd behavior leads to a self-approving circle of papers on a subject of little practical significance. Real progress usually comes from a succession of incremental and progressive results, as opposed to those that feature only variations on a problem’s theme.

At Bell Labs, the mathematician Richard Hamming used to divide his fellow researchers into two groups: those who worked behind closed doors and those whose doors were always open. The closed-door people were more focused and worked harder to produce good immediate results, but they failed in the long term. Today I think we can take the open or closed door as a metaphor for researchers who are actively connected and those who are not. And just as there may be a right amount of networking, there may also be a right amount of reading, as opposed to writing. Hamming observed that some people spent all their time in the library but never produced any original results, while others wrote furiously but were relatively ignorant of the relevant literature.

Hamming, who shared an office with Claude Shannon and knew many famous
scientists and engineers, also remarked on what he saw as a "Nobel Prize effect," where once having achieved a famous result, a researcher felt that he or she could work only on great problems, consequently never doing great work again. From small-problem acorns, great trees of research grow.

Like a lot of things in life, it helps to be in the right place at the right time. Sometimes all the good and well-intentioned advice in the world won't help you avoid working on a dead-end problem. I know—I've been there, done that.
President Barack Obama arrived in Lawrenceville this morning for a tour of Carnegie Mellon University's robotics center.

Traffic was shut down on the Parkway West starting around 9:45 a.m. as the president's motorcade traveled through town.

Some people stopped Downtown to watch as he went by, including, given their outfits, some of the people attending the furry convention here.

Mr. Obama arrived at the robotics center at 10:15 a.m.

People along Lawrenceville's narrow streets poked their heads out of second and third story windows as the motorcade passed.

Mr. Obama was greeted by a few protesters.

Imagining advances ranging from lighter cars to smarter robots, Mr. Obama is announcing a $500 million project to spur high-technology manufacturing, a sector of U.S. industry that presidential advisers say has lost ground to such competitors as Germany and Japan.

Today in Pittsburgh, Mr. Obama is to call for a joint effort by industry, universities and the federal government to help reposition the United States as a leader in cutting-edge manufacturing, including biotechnology, robotics and nanotechnology -- the development of new materials at the molecular level.

The initiative represents yet another effort by Mr. Obama to promote job-creation in the midst of an economic slowdown that has reduced hiring and weakened his job approval standing with the public. The president has tried to elevate his profile on the economy with weekly job-related trips to states that are key to his re-election.

He is launching his new high-tech plan at Carnegie Mellon, one of six universities in what the administration is calling the Advanced Manufacturing Partnership. The plan also features 11 manufacturing companies, including Ford Motor Co., Caterpillar Inc., Procter & Gamble Co. and Northrop Grumman Corp. Leading the effort will be Andrew
Liveris, chairman, president and CEO of the Dow Chemical Co., and Susan Hockfield, president of the Massachusetts Institute of Technology.

"The idea here is that we're bringing together all of the key players in a collaborative partnership to help identify these promising technologies, to invest in these promising technologies and to use them to drive a revitalization of American manufacturing," said Ron Bloom, assistant to the president for manufacturing policy.

Mr. Obama is touring the Carnegie Mellon Robotics Institute, which is building machines that can help with bomb disposal, brain surgery, lawn mowing and paint scraping. Ultimately, some scientists at the institute are trying to figure out whether robots and humans can "treat each other as equal partners or teammates."

The administration's plan includes $70 million for a robotics initiative. It also is aiming $300 million toward national security industries and $100 million for research and training to more quickly develop advanced materials at lower costs. Some of the $500 million would come from existing allocations to government agencies, but other money is only reflected in Mr. Obama's 2012 budget request and would require approval by Congress.