

Index

Cyber Bytes - 10 JUN 11

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

Links of interest:

CNBC's special on the cyber security threat to America, "Code Wars": <http://www.cnn.com/id/42210831/>

CSBA's *The Maturing Revolution in Military Affairs* report: <http://www.csbaonline.org/publications/2011/06/the-maturing-revolution-in-military-affairs/>

Center for a New American Security's two part report on U.S. Cyber Security Strategy: <http://www.cnas.org/node/6456>

World IPv6 Day: <http://www.worldipv6day.org/> and <http://server9.test-ipv6.com/ipv6day.html>

Apple to Build "Mini-Pentagon"-like Headquarters (or a "Mothership") [video]: <http://techcrunch.com/2011/06/07/steve-jobs-cupertino/>

Cyber Security

Data Breach at Security Firm Linked to Attack on Lockheed
-<http://www.nytimes.com/2011/05/28/business/28hack.html?_r=1>

Lockheed Martin Cyber Attack: Routine, a Warning or a Possible Act of War?
-<http://spectrum.ieee.org/riskfactor/telecom/security/lockheed-martin-cyber-attack-routine-a-warning-or-a-possible-act-of-war?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrumMilitary+%28IEEE+Spectrum%3A+Military%29>

Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks
-<<http://www.wired.com/threatlevel/2011/05/l-3/>>

Digital Ants Protect Computer Networks
-<<http://news.wfu.edu/2011/05/27/digital-ants-protect-computer-networks/>>

Google Mail Hack Blamed on China
-<<http://online.wsj.com/article/SB10001424052702303657404576359770243517568.html>>

Index

US Weighs Security After 'Serious' Google Allegation

-<[Can Google Know Where the gMail Attack Came From?](http://news.yahoo.com/s/nm/20110602/tc_nm/us_google_clinton;_ylt=AtNpxQA5kDCj03AfUuKD1Z9T.3QA;_ylu=X3oDMTJua2prZmNvBGFzc2V0A25tLzlwMTEwNjAyL3VzX2d2vb2dsZV9jbGludG9uBHBvcwM0BHNIYwN5bl9wYWdpbmF0ZV9zdW1tYXJ5X2xpc3QEc2xrA3Vzd2VpZ2hzc2VjdQ--></p></div><div data-bbox=)

-<<http://www.technologyreview.com/web/37698/?ref=rss&a=f>>

Pinning Hacking Blame on China Could Be Tough: CNO

-<<http://www.reuters.com/article/2011/06/02/us-usa-defense-cyber-idUSTRE7517G820110602>>

Cyber Spies Target Chinese Experts

-<<http://online.wsj.com/article/SB10001424052702304563104576363743171105376.html>>

China Linked to New Breaches Tied to RSA

-<http://news.cnet.com/8301-27080_3-20068836-245/china-linked-to-new-breaches-tied-to-rsa/?part=rss&subj=news&tag=2547-1_3-0-20>

Security 'Tokens' Take Hit

-<<http://online.wsj.com/article/SB10001424052702304906004576369990616694366.html>>

RSA to Replace SecurID Tokens Following Breaches

-<http://news.cnet.com/8301-1009_3-20069632-83/rsa-to-replace-securid-tokens-following-breaches/?part=rss&tag=feed&subj=News-Security>

US Military, Businesses Seek Better Defenses on the Inside

-<<http://www.technologyreview.com/business/37678/?ref=rss>>

Anonymous Warns NATO Not to Challenge It

-<http://news.cnet.com/8301-1009_3-20070283-83/anonymous-warns-nato-not-to-challenge-it/?part=rss&subj=news&tag=2547-1_3-0-20>

Navy Rolls Out Regional Cybersecurity Centers

-<<http://defensesystems.com/articles/2011/06/09/naval-it-day-deets-network-cybersecurity.aspx>>

Citi Data Theft Points Up a Nagging Problem

-<<http://www.nytimes.com/2011/06/10/business/10citi.html?>

Index

[_r=1&partner=rss&emc=rss>](#)

Few Cyberattacks Are Cause for Major Retaliation

[-<http://www.networkworld.com/news/2011/060811-experts-few-cyberattacks-are-cause.html>](http://www.networkworld.com/news/2011/060811-experts-few-cyberattacks-are-cause.html)

Cyber War

Cyber Combat: Act of War

[-<http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>](http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html)

UK Developing Cyber-Weapons Programme to Counter Cyber War Threat

[-<http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive>](http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive)

List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare

[-<http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSubIFH_story.html>](http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSubIFH_story.html)

Could a Cyber War Turn Into a Real One for the US?

[-<http://www.reuters.com/article/2011/06/01/us-usa-cyber-pentagon-idUSTRE74U75420110601>](http://www.reuters.com/article/2011/06/01/us-usa-cyber-pentagon-idUSTRE74U75420110601)

The Pentagon Is Confused on How to Fight a Cyber War

[-<http://www.theatlanticwire.com/technology/2011/06/pentagon-confused-about-how-fight-cyber-war/38357/>](http://www.theatlanticwire.com/technology/2011/06/pentagon-confused-about-how-fight-cyber-war/38357/)

US Aims Missiles at Hackers

[-<http://www.technologyreview.com/web/37692/?ref=rss&a=f>](http://www.technologyreview.com/web/37692/?ref=rss&a=f)

Chinese Military Scholars Accuse US of Launching 'Internet War'

[-<http://www.npr.org/blogs/thetwo-way/2011/06/03/136923033/chinese-military-scholars-accuse-u-s-of-launching-internet-war?ft=1&f=1001>](http://www.npr.org/blogs/thetwo-way/2011/06/03/136923033/chinese-military-scholars-accuse-u-s-of-launching-internet-war?ft=1&f=1001)

Latest Hacks Could Set the Stage for Cyberwar [audio]

[-<http://www.npr.org/2011/06/06/137000302/latest-hacks-could-set-the-stage-for-cyberwar?ft=1&f=1001>](http://www.npr.org/2011/06/06/137000302/latest-hacks-could-set-the-stage-for-cyberwar?ft=1&f=1001)

DoD

Information Dominance, Naval Intelligence Welcome New Leadership

Index

Marine Corps Aviators Depend Upon iPad

-<<http://www.tuaw.com/2011/05/31/marine-corps-aviators-depend-on-ipad/>>

Is Stealth Dead?

-<<http://www.dodbuzz.com/2011/06/03/is-stealth-dead/>>

China, Russia Could Make US Stealth Tech Obsolete

-<<http://www.wired.com/dangerroom/2011/06/stealth-tech-obsolete/>>

Killer App: Army Tests Smartphones for Combat

-<<http://online.wsj.com/article/SB10001424052702304563104576361480888426472.html>>

Navy Should Wait to Implement UCore (Universal Core) [Data Strategy]

-<http://www.fierceregovernmentit.com/story/rand-navy-should-wait-implement-ucore/2011-06-07?utm_medium=rss&utm_source=rss>

Navy Focuses on IT Efficiency: 'Overarching' Networking Strategy On Hold

'Ruthless' Cost Cutting Coming to Navy IT

-<<http://www.federalnewsradio.com/?sid=2415607&nid=35>>

Navy Needs a Way to Handle UAV, Sensor Data

-<<http://defensesystems.com/articles/2011/06/09/naval-it-day-afcea-tcped-intelligence-data-challenge.aspx>>

Marines Buying \$880 Million Worth of PCs, Laptop and Tablet Computers

-<http://www.nextgov.com/nextgov/ng_20110608_5109.php>

Information & Society

China's PLA Bans Soldiers from Social Media

-<<http://www.defensenews.com/story.php?i=6683857&c=POL&s=TOP>>

US Navy Calls On Video Gamers for Strategic Help

-<http://www.pbs.org/newshour/extra/features/us/jan-june11/navygame_06-01.html>

Army Seeks Social Media Gurus to Save Afghan War

-<<http://www.wired.com/dangerroom/2011/06/army-seeks-social-media-gurus-to-save-the-afghan-war/>>

Index

Information Technology

Data Grows, and So Do Storage Sites

-<http://www.nytimes.com/2011/06/06/technology/internet/06dropbox.html?_r=2>

Intel, Apple & the Transformation of the PC

-<<http://www.patentlyapple.com/patently-apple/2011/06/intel-apple-the-transformation-of-the-pc.html>>

Which Hot Tech Companies Are Winning the Fight for Top Coders?

-<<http://www.wired.com/epicenter/2011/06/talent-fight-silicon-valley/>>

Happy IPv6 Day

-<<http://bits.blogs.nytimes.com/2011/06/08/happy-ipv6-day/?partner=rss&emc=rss>>

Google, Microsoft, and Yahoo Team Up to Advance Semantic Web

-<<http://www.technologyreview.com/web/37765/?ref=rss&a=f>>

Robotics

DARPA Concludes Nano Air Vehicle Program, We Wonder What's Next [video]

-<http://spectrum.ieee.org/automaton/robotics/military-robots/darpa-concludes-nano-air-vehicle-program-we-wonder-whats-next?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IEEE+Spectrum+%28IEEE+Spectrum%29>

Pentagon's Drone Surge Includes \$5.3 Billion for General Atomics

-<<http://about.bgov.com/2011/05/31/pentagon's-drone-surge-includes-5-3-billion-for-general-atomics/>>

DoD Testers Slam Global Hawk

-<<http://www.dodbuzz.com/2011/06/07/report-dod-testers-slam-global-hawk/>>

Space

GAO: DoD Space Acquisitions Threatened by Poor Oversight

-<http://www.fierceregovernmentit.com/story/gao-dod-space-acquisitions-threatened-poor-oversight/2011-06-01?utm_medium=rss&utm_source=rss>

Index

Technology Advancements

5 Technologies That Will Shape the Web

-<<http://spectrum.ieee.org/telecom/internet/5-technologies-that-will-shape-the-web/0>>

Helping Chips Sip Power

-<[http://online.wsj.com/article/](http://online.wsj.com/article/SB10001424052702304906004576367513123434574.html)

SB10001424052702304906004576367513123434574.html

First Graphene Integrated Circuit

-<[http://spectrum.ieee.org/semiconductors/devices/first-graphene-integrated-circuit?](http://spectrum.ieee.org/semiconductors/devices/first-graphene-integrated-circuit?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ieeeSpectrum+%28IEEE+Spectrum%29)

utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A

+ieeeSpectrum+%28IEEE+Spectrum%29>

Data Breach at Security Firm Linked to Attack on Lockheed

Data Breach at Security Firm Linked to Attack on Lockheed

By [CHRISTOPHER DREW](#) and [JOHN MARKOFF](#)

Published: May 27, 2011

[Lockheed Martin](#), the nation's largest military contractor, has battled disruptions in its computer networks this week that might be tied to a hacking attack on a vendor that supplies coded security tokens to millions of users, security officials said on Friday.

The SecurID electronic tokens, which are used to gain access to computer networks by corporate employees and government officials from outside their offices, are supplied by the RSA Security division of the EMC Corporation.

RSA acknowledged in March that it had sustained a data breach that could have compromised some of its security products. Executives in the military industry said Friday that Lockheed's problems appeared to stem from that data breach and could be the first public signs of damage from it.

The March intrusion reverberated through the computer security community. The RSA technology is used by most Fortune 500 companies and federal agencies to provide an extra layer of security when employees use their networks from customer offices, hotels or their homes.

Many of RSA's customers have taken extra measures since the intrusion was discovered, either by adding security measures, finding alternative solutions or simply shutting off remote access. Security experts said it was possible that companies other than Lockheed had faced attacks, whether they realized it or not.

"The issue is whether all of the security controls are compromised," said James A. Lewis, a senior fellow and a specialist in computer security issues at the Center for Strategic

Data Breach at Security Firm Linked to Attack on Lockheed

and International Studies, a policy group in Washington. “That’s the assumption people are making.”

Neither RSA, which is based in Bedford, Mass., nor Lockheed would discuss the problems on Friday.

Officials in the military industry, who spoke only on the condition of anonymity given the sensitivity of the matter, said Lockheed had detected an intruder trying to break into its networks last Sunday. It shut down much of its remote access and has been providing new tokens and passwords to many workers, company employees said.

Lockheed makes fighter planes, spy satellites and other confidential equipment. It also sells cybersecurity services to military and intelligence agencies, and some experts said its failure to take greater precautions with its own systems could be embarrassing.

“We don’t know what they went after at Lockheed,” Mr. Lewis said, referring to the hackers behind the intrusion attempt. “One possibility is that it’s a state actor, but it could also be criminals who are trying to exploit the company’s customers.”

Industry officials said military contractors, who are bombarded daily by hacking attempts, typically do not keep classified data on computers that can be entered remotely. Federal authorities have said that China, Russia and other countries sponsor hackers trying to ferret out American military and corporate secrets.

Raytheon, another large military contractor, issued a statement on Friday saying that it took “immediate companywide actions” when the RSA breach was disclosed in March. “As a result of these actions,” the company said, “we prevented a widespread disruption of our network.”

General Dynamics said it had not had any problems related to the breach. Other giant

Data Breach at Security Firm Linked to Attack on Lockheed

military contractors, like Northrop Grumman and Boeing, declined to comment.

Jeffery Adams, a spokesman for Lockheed, said the company would not publicly discuss specific threats or its responses.

“However, to counter any threats, we regularly take actions to increase the security of our systems and to protect our employee, customer and program data,” he said in a statement. “We have policies and procedures in place to mitigate the cyberthreats to our business, and we remain confident in the integrity of our robust, multilayered information systems security.”

Security experts said companies in many industries had increased network monitoring or changed passwords and PINs for the tokens since the RSA breach.

But some of the specialists said that until more details were known, it remained possible that the attempted intrusion at Lockheed was not tied to the RSA breach.

The RSA tokens provide security beyond a user name or password by requiring users to append a unique number generated by the token each time they connect to their corporate or government networks.

Soon after the breach in March, RSA’s chairman, Art Coviello, said the company’s investigation had revealed that the intruder successfully stole digital information from the company that was related to RSA’s SecurID products.

He did not give precise details about the nature of the information but said it could potentially reduce the effectiveness of the system in the face of a “broader attack.” The company said then that there was no indication that the information had been used to attack its customers.

Data Breach at Security Firm Linked to Attack on Lockheed

Some computer security specialists said at the time that the compromised information was a file of master keys — long numbers — that are a part of the RSA encryption system. If the intruder did gain those numbers, it would make it possible to fashion an attack based on independently generating the keys used by individual customers.

RSA officials have said that the intrusion was only partly successful.

Mr. Lewis, the security specialist at the Center for Strategic and International Studies, said the intruders had been detected as they were trying to transfer data by security software provided by the NetWitness Corporation, a company that provides network monitoring software. In April, NetWitness was acquired by RSA's parent company, EMC.

Lockheed Martin Cyber Attack: Routine, a Warning or a Possible Act of War?

Lockheed Martin Cyber Attack: Routine, a Warning or a Possible Act of War?

POSTED BY: ROBERT CHARETTE / TUE, MAY 31, 2011

Last Thursday, [Reuters](#) ran a story that the US defense firm [Lockheed Martin](#) was experiencing a major disruption to its computer systems because of cyber attack.

The Reuters story said that the attack began the weekend before and indicated that it involved the company's [SecurID tokens](#) which allow Lockheed's 126,000 employees "... to access Lockheed's internal network from outside its firewall."

As a result of the attack, Lockheed reset all of its employees' passwords.

You may recall that last March, SecurID, the major two-factor authentication security product of [RSA](#) (which is the security division of the [EMC Corporation](#)), was itself the target of a sophisticated cyber attack. The attack resulted in SecurID's offering to be partially compromised. SecurID is used by 40 million people and 30,000 organizations worldwide.

In the wake of the attack on SecurID, Lockheed took steps to increase its IT security defenses and lower its reliance on SecurID, as did many other defense and commercial companies. [Steve Winterfeld](#), cyber technical lead at defense contractor [TASC](#) which is deeply involved in IT security, was quoted as saying in the Reuters article:

"You have no idea how many people are freaked out right now [about the SecurID breach] ... TASC is no longer treating the RSA device as if it were as secure as it was beforehand."

The Reuters article started a media feeding frenzy of speculation about what was going on at Lockheed and whether US defense secrets were at risk. The \$45.8 billion company makes the [F-22](#) and [F-35](#) stealth fighters, among many, many other classified defense systems.

Lockheed Martin Cyber Attack: Routine, a Warning or a Possible Act of War?

Helping confirm the story was that Reuters used an unnamed defense official as a major source of its information, as well as two other sources who also declined to be identified. Lockheed also wasn't immediately forthcoming about what was going on, nor was SecurID. And a US defense official deciding to go public with the information seemed to indicate that the US Department of Defense wasn't happy about what was going on at Lockheed.

The Reuters story - and further speculation that US defense secrets may have been taken not only at Lockheed Martin, but other defense contractors like Boeing, Northrop Grumman and Raytheon among others - spread like wildfire, which then caused Lockheed to issue a press release late Friday that stated:

"On Saturday, May 21, Lockheed Martin detected a significant and tenacious attack on its information systems network. The company's information security team detected the attack almost immediately, and took aggressive actions to protect all systems and data. As a result of the swift and deliberate actions taken to protect the network and increase IT security, our systems remain secure; no customer, program or employee personal data has been compromised."

"Throughout the ongoing investigation, Lockheed Martin has continued to keep the appropriate U.S. government agencies informed of our actions. The team continues to work around the clock to restore employee access to the network, while maintaining the highest level of security."

So, was the cyber attack routine - Lockheed, like most government and commercial defense organizations around the world, gets attacked on a daily basis - or was it something more? The jury is still out, but there does seem to be a sense that the SecurID breach may be more significant than first thought. SecurID is still not talking about the Lockheed issue, at least not yet.

The Financial Times of London today had a nice explanation of why the IT security community is uneasy about what happened at Lockheed:

"The National Security Agency ...[declared that] ... not long after the RSA attack that the

Lockheed Martin Cyber Attack: Routine, a Warning or a Possible Act of War?

tokens should no longer be deemed sufficient to grant access to 'critical infrastructure'. Defence contractors including Lockheed began requiring employees to put in extra personal passwords."

"Although Lockheed said its programs and customer data had not been compromised in the attack, the breach suggests that the extra passwords were not sufficient to repel hackers, an ominous sign for remote-access systems in defence and other industries."

The Lockheed cyber attack also suggests that it isn't some lone hacker that was involved in the SecurID breach, but more likely a state-sponsored group. Lockheed has some of the most sophisticated IT security defenses around, and it is unlikely that a single hacker would have been able to cause as much disruption to Lockheed's network as has been reported.

Last March, EMC played down the financial impact of the cyber attack on SecurID. That may now be changing.

Raising the story's profile a bit more, there is also a story in today's Wall Street Journal reporting that the US government has decided that certain types of cyber attacks originating from another country can constitute an act of war, and therefore trigger a "traditional" military response from the US.

As one military official in the WSJ article stated it:

"If you shut down our power grid, maybe we will put a missile down one of your smokestacks."

Of course, tracking such an attack as being sponsored by specific country is not especially easy, as this other Reuters story from yesterday points out. And if Lockheed's IT systems had been significantly compromised say by another country, would that warrant US military retaliation?

A story in The Australian says that Australian mining companies are experiencing an onslaught of cyber attacks by persons unknown who are seemingly interested in gaining insights into their corporate decision making and strategic plans. Do cyber

Lockheed Martin Cyber Attack: Routine, a Warning or a Possible Act of War?

attacks that target a country's economic interests constitute an act of war?

What if a major US bank's IT systems were taken out, say in similar fashion to what [happened to South Korea's Nonghyup bank](#) by supposedly North Korea?

And how long does a power grid have to be turned off by a cyber attack to start a war?
An hour, a day or a week or more?

The WSJ says that the decision to treat certain types of cyber attacks as potential acts of war is part of a DoD cyber strategy policy document which is expected to be made public in the following weeks. I will be interested whether it has answers to these types of questions or not.

Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks

Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks

By [Kevin Poulsen](#)   May 31, 2011 | 4:11 pm

An executive at defense giant L-3 Communications warned employees last month that hackers were targeting the company using inside information on the SecurID keyfob system freshly stolen from an acknowledged breach at RSA Security.

The L-3 attack makes the company the second hacker target linked to the RSA breach — both defense contractors. Reuters reported Friday that [Lockheed Martin had suffered an intrusion](#).

“L-3 Communications has been actively targeted with penetration attacks leveraging the compromised information,” read an April 6 e-mail from an executive at L-3’s Stratus Group to the group’s 5,000 workers, one of whom shared the contents with [Wired.com](#) on condition of anonymity.

It’s not clear from the e-mail whether the hackers were successful in their attack, or how L-3 determined SecurID was involved. L-3 spokeswoman Jennifer Barton declined comment last month, except to say: “Protecting our network is a top priority and we have a robust set of protocols in place to ensure sensitive information is safeguarded. We have gotten to the bottom of the issue.” Barton declined further comment Tuesday.

Based in New York, [L-3 Communications](#) ranks eighth on [Washington Technology’s 2011 list](#) of the largest federal-government contractors. Among other things the company provides command-and-control, communications, intelligence, surveillance and reconnaissance (C3ISR) technology to the Pentagon and intelligence agencies.

In the Lockheed breach, attackers may have gained access by cloning the SecurID

Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks

keyfobs of Lockheed users.

Together, the attacks suggest the RSA intruders obtained crucial information — possibly the encryption seeds for SecurID tokens — that they're using in targeted intelligence-gathering missions against sensitive U.S. targets.

The attacks come as the Pentagon is in the final stages of [formalizing a doctrine](#) for military operations in cyberspace, which will reportedly view cyberattacks that cause death or significant real-world disruption as the equivalent of an armed attack.

RSA Security, a division of EMC, declined to comment on the L-3 incident.

SecurID adds an extra layer of protection to a login process by requiring users to enter a secret code number displayed on a keyfob, or in software, in addition to their password. The number is cryptographically generated and changes every 30 seconds.

RSA acknowledged in March that it had been the [victim of an “extremely sophisticated” hack](#) in which intruders succeeded in stealing information related to the company's SecurID two-factor authentication products.

“While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers,” RSA wrote at the time, “this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack. We are very actively communicating this situation to RSA customers and providing immediate steps for them to take to strengthen their SecurID implementations.”

RSA characterized the breach as an “advanced persistent threat,” or APT. APT is a buzzword assigned to unusually sophisticated attacks in which intruders use social engineering coupled with zero-day vulnerabilities to infiltrate a target network at a

Second Defense Contractor L-3 'Actively Targeted' With RSA SecurID Hacks

weak point, and then spread out carefully to steal source code and other intellectual property. Last year's hack into Google was considered an APT attack and — like many intrusions in this category — was linked to China.

L-3 uses SecurID for remote employee access to the unclassified corporate network, but classified networks at the company would not have been at risk in the attack, the L-3 source said.

Asked if the RSA intruders did gain the ability to clone SecurID keyfobs, RSA spokeswoman Helen Stefen said, “That’s not something we had commented on and probably never will.”

If the intruders have gained cloning ability, the implications could be far-reaching. SecurID is used by most federal agencies and Fortune 500 companies. As of 2009, RSA counted 40 million customers carrying SecurID hardware tokens, and another 250 million using software clients.

RSA has been privately briefing its customers about its intrusion, but only after placing them under nondisclosure agreements, and the company has shared few details with the public.

Digital Ants Protect Computer Networks

Digital ants protect computer networks

By KERRY M. KING ('85) *Office of Communications and External Relations*

As the nation's electrical power grid becomes more interconnected through the Internet — from the nuclear power plant in California to transmission lines in Texas to the microwave in your kitchen — the chances of cyber attacks increase as well.

Professor of Computer Science Errin Fulp is training an army of “digital ants” to turn loose into the power grid to seek out computer viruses trying to wreak havoc on the system.

If the approach proves successful in safeguarding the power grid, it could have wide-ranging applications on protecting anything connected to SCADA (Supervisory Control and Data Acquisition) networks, computer systems that control everything from water and sewer management systems to mass transit systems to manufacturing systems.

Fulp is working this summer with scientists at Pacific Northwest National Laboratory (PNNL) in Richland, Wash., on the next steps in the digital ants technology, developed by PNNL and Wake Forest over the last several years. The approach is so promising that it was named one of the “ten technologies that have the power to change our lives,” by Scientific American magazine last year.

The power grid is probably more vulnerable to cyber attacks than security experts would like to admit, said Fulp, an expert in security and computer networks. As the grid becomes more and more interconnected, it offers hackers more points to enter the system; for instance, inserting a virus or computer worm into a low security site, such as

Digital Ants Protect Computer Networks

in your home's smart grid, to gain access to more secure systems up the line.

“When that network connects to a power source, which connects to the smart grid, you have a jumping off point” for computer viruses, he said. “A cyber attack can have a real physical result of shutting off power to a city or a nuclear power plant.”

The digital ants technology could transform cyber security because it adapts rapidly to changing threats, said Fulp, who has received nearly \$250,0000 in grants from PNNL/Battelle Memorial Institute for his ongoing research.

Unlike traditional security approaches, which are static, digital ants wander through computer networks looking for threats such as computer worms, self-replicating programs designed to steal information or facilitate unauthorized use of computers. When a digital ant detects a threat, it summons an army of ants to converge at that location, drawing the attention of human operators to investigate.

“The idea is to deploy thousands of different types of digital ants, each looking for evidence of a threat,” Fulp said. “As they move about the network, they leave digital trails modeled after the scent trails ants in nature use to guide other ants. Each time a digital ant identifies some evidence, it is programmed to leave behind a stronger scent. Stronger scent trails attract more ants, producing the swarm that marks a potential computer infection.”

The concept has proven successful in testing on a small scale, but will it still work when it's scaled up to protect something as large and complex as the nation's power grid? Fulp and two of his students — computer science graduate students Michael Crouse and Jacob White — are working this summer with scientists at PNNL and from the University of California at Davis to answer that question. But even using PNNL's vast computer platforms, they can only rely on computer simulations to predict the ants'

Digital Ants Protect Computer Networks

“behavior” up to a point.

That’s where Associate Professor of Mathematics Ken Berenhaut, an expert in mathematical modeling and simulation, comes in. Berenhaut, along with graduate student Ross Hilton, will use modeling to help determine what will happen as the ants move about the smart grid from the hot water heater in your house to the electrical substation to the power plant.

Among the questions to be answered: How do the ants migrate across different computer platforms and systems operating at different speeds? How many ants should you have patrolling a system? How long do they live? How do the ants scale up to identify a threat and then ramp back down?

“In nature, we know that ants defend against threats very successfully,” Fulp said. “They can ramp up their defense rapidly, and then resume routine behavior quickly after an intruder has been stopped. We’re trying to achieve that same framework in a computer system.”

PNNL, a Department of Energy laboratory, conducts cutting-edge research in cyber security. Glenn Fink, a senior research scientist at PNNL, first came up with the idea of copying ant behavior for computer security. He was familiar with Fulp’s work developing faster computer scans using parallel processing — dividing computer data into batches like lines of shoppers going through grocery store checkouts, where each lane is focused on certain threats — and invited him to join the project several years ago.

Fulp and two of his students, Wes Featherstun (’08, MS ’10) and Brian Williams (’08, MS ’10), then graduate students in computer science, worked at PNNL during the summer of 2009. Fulp and Crouse worked there again last summer.

Digital Ants Protect Computer Networks

Google Mail Hack Blamed on China

Google Mail Hack Blamed on China

By [AMIR EFRATI](#) And [SIOBHAN GORMAN](#)

[Google](#) Inc. said Chinese hackers targeted the email accounts of senior U.S. officials and hundreds of other prominent people in a fresh computer attack certain to intensify growing concern about the security of the Internet.

The victims, including government and military personnel, Asian officials, Chinese activists and journalists, were tricked into sharing their Gmail passwords with "bad actors" based in China, Google said in an unusual blog post. The attack's goal was to read and forward the victims' email.

Google said hundreds of Gmail users were tricked into sharing their passwords with "bad actors" based in China, potentially further complicating its relations with the country. Don Clark has details.

The company, which in 2010 blamed China for an attack on its computer networks, said it recently discovered the Gmail campaign, which "appears to originate from Jinan, China," and targeted specific individuals.

In Washington, the Federal Bureau of Investigation and Department of Homeland Security said they were working with Google to investigate the attacks. "We have no reason to believe that any official U.S. government email accounts were accessed," said Caitlin Hayden, a spokeswoman for the National Security Council.

Jinan, a large city about 250 miles south of Beijing, is home to one of the People's Liberation Army's technical reconnaissance bureaus, which serve as arms of China's equivalent of the National Security Agency, according to a 2009 report from a committee created by Congress to study China.

Google Mail Hack Blamed on China

A Difficult Search

[View Interactive](#)



Since its entry into the Chinese-language world in 2000, U.S. search giant Google Inc. has struggled to balance its growth ambitions in the vast but restrictive new market while adhering to a self-held principle: "Don't be evil."

The goal of the latest hijacking campaign "seems to have been to monitor the contents of the these users' emails" wrote Eric Grosse, an engineering director on Google's security team, in Wednesday's blog post. He said Google's system wasn't hacked, rather users were duped. He said the company notified victims of the hijackings, secured their accounts and "notified relevant government authorities."

Google, which claims more than 200 million users for its free, Web-based Gmail email service, declined to comment on the identities of the affected individuals, how it traced the attacks to Jinan or who may be behind the incident.

The latest attack continues a troubling wave of incidents involving corporate and government computer networks, which have exposed private information of millions users and raised fears about the safety of government secrets. Last week, defense contractor [Lockheed Martin Corp.](#) said it had detected a significant attack against its computer networks.

A Microsoft Corp. spokesman said the company wasn't aware of any similar

Google Mail Hack Blamed on China

attacks targeting the customers of its Hotmail email service, but added "phishing attacks are a persistent industry challenge." A Yahoo Inc. spokeswoman declined to comment on whether Yahoo users were similarly targeted but said "we take security very seriously and we would take appropriate action in the event of any kind of breach."

Google's latest disclosure didn't mention the possibility of involvement by the government of China. Google's systems have been repeatedly targeted by Chinese hackers since the successful attack in December 2009, said a person familiar with the matter. Chinese officials have denied any connection to attacks on Google or other companies.

By disclosing the latest attacks originated in Jinan and targeted U.S. officials, Chinese human-rights activists and other people "who would only be of interest to the Chinese government," it appears "Google is pointing their finger at them," said Alex Stamos, chief technology officer at security firm iSEC Partners.

Jinan is also home to the Shandong Jinan Lanxiang Vestibule School, a vocational school that teaches computer training. The school has been a source of past attempts to launch targeted email attacks on a defense contractor, said James Mulvenon, a cybersecurity specialist who focuses on China.

Big Phish

Google says a scam based in China tricked some Gmail users. Here is how it worked:

Victim receives email that seems to come from a close associate or colleague

Message appears to have an attachment with link that leads to a fake Gmail login page; user's password is stolen when it is typed into site

Attacker can use password to forward incoming Gmail messages to another account, read the mail and gather personal information for more attacks

The school at one point held the Guinness world record for having the

Google Mail Hack Blamed on China

largest number of people online, Mr. Mulvenon noted. "If I were looking for a place to use as cover [for an attack], this would be a good place," he said.

A woman who answered the phone in the administrative office of the school said the issue had nothing to do with the school.

In response to the 2009 attack, Google in 2010 moved its mainland Chinese search service to Hong Kong and stopped obeying the Chinese government's requirement to censor results, which Google had been following since 2006. China's own Internet filters now censor Google's searches for users in China.

Eric Schmidt, Google's chairman, said Tuesday the company has made improvements to its security systems since the 2009 attack. "Google is massively more protected than we were a year ago," he said, during an interview at the The Wall Street Journal's "D9: All Things Digital" conference.

Mr. Schmidt said Google had discovered "lots of other companies were attacked in similar ways," suggesting many firms don't report such incidents. "It is better to be transparent about these things," he said.

Google's latest blog post said that to uncover the phishing campaign, the company partly relied on a public blog post by an independent researcher, Mila Parkour, who wrote in February that Gmail users were being targeted and posted examples.

In a post on Feb. 17 on her website, called Contagio Malware Dump, Ms. Parkour wrote that the attack "is far from being new or sophisticated" but she wanted to post information about it "due to the particularly invasive approach."

Journal Community

Victims of the attack received "spoof" emails from what appeared to be their

Google Mail Hack Blamed on China

trusted contacts or employees of the U.S. State Department or Defense Department, she said. The emails had links to a fake Gmail login page that the scammers used to collect the users' passwords once they tried to log in again.

The targeted recipients were "government and non government employees working on questions of defense, political affairs, national security, defense/military personnel," she said, adding the campaign began more than a year ago.

Phishing attacks account for about 20% to 30% of email hijackings, estimated Mr. Stamos. "Spear phishing," which targets specific individuals, is harder for companies to detect, he added. He expects Gmail's new security upgrades, which help prevent such attacks by letting Google recognize the user's primary mobile device or computer that is used to access the account, will become a standard among online email providers.

—Geoffrey A. Fowler and Nick Wingfield contributed to this article.

Read more: <http://online.wsj.com/article/SB10001424052702303657404576359770243517568.html#ixzz1O7jKaYd2>

US Weighs Security After 'Serious' Google Allegation

U.S. weighs security after "serious" Google allegation

By Andrew Quinn – Thu Jun 2, 2:55 pm ET

WASHINGTON (Reuters) – Washington scrambled on Thursday to assess whether security had been compromised after Google Inc revealed a major hacker attack targeting U.S. officials that the Internet giant pegged to China.

"These allegations are very serious," Secretary of State Hillary Clinton said.

"We take them seriously; we're looking into them," Clinton told reporters a day after the Internet giant said it had disrupted a campaign aimed at stealing passwords of hundreds of Google email account holders, including senior U.S. government officials, Chinese activists and journalists.

Google's announcement fuels debate in Washington over China's intentions in cyberspace, which the United States has identified as a potential flashpoint for future conflict.

Blackberry maker Research In Motion and Microsoft Corp. could get a boost from the Google hacking incident. The companies have been fending off competitive challenges from Google's Android software and cloud computing services, as the corporate sector and the federal government explore whether Google is a secure alternative for email.

Neither Google nor the U.S. government has said the Chinese government was behind the attacks, and the U.S. State Department said it had not raised the issue with Beijing.

Google only said the attack appeared to originate in China.

Beijing nevertheless reacted angrily to Google's charge, saying it was "unacceptable" to blame Beijing and allegations that China supports hacking "have ulterior motives".

US Weighs Security After 'Serious' Google Allegation

Clinton said Google told the State Department before it made its public announcement on Wednesday, and the U.S. Federal Bureau of Investigation was investigating, with Google.

The White House said it had no reason to believe official government emails were hacked in the Google incident, and officials at many agencies stressed that government employees were directed not to use private accounts to discuss sensitive issues.

"Rule number one is: don't do anything stupid," one national security official said.

Some agencies, including the Securities and Exchange Commission and the Commodity Futures Trading Commission, block employees from accessing personal accounts from work. But there is no blanket ban and other agencies do allow it.

"Those of us who do run private accounts are very, very mindful of the security issues," Chief of Naval Operations Admiral Gary Roughead told Reuters.

Still, the government will check whether senior officials' private accounts were targeted, said one official, speaking on condition of anonymity.

"There is a lot of awareness that whether it's a hostile intelligence service or others who may want to access this," the official said.

DUELING IN CYBERSPACE

Google's latest salvo looked likely to bring Internet policy to the foreground in the U.S.-China relationship, where Washington and Beijing have staked out sharply contrasting approaches to censorship, freedom of speech and cybersecurity.

The United States was drawn in last year when Google temporarily shut its Chinese-language portal over censorship concerns and a cyber attack it said was traced to China. Clinton also has accused Beijing of facing a "dictator's dilemma" as it seeks to

US Weighs Security After 'Serious' Google Allegation

control technologies that are fueling growth and free speech around the world.

The dispute over the Internet has at times amplified existing strains in the U.S.-China relationship on everything from human rights and trade to intellectual property rights.

The United States has warned that a devastating cyberattack could result in real-world military retaliation, although analysts say it could be difficult to detect its origin with full accuracy.

The White House and the State Department have appointed officials to oversee cybersecurity issues.

The Pentagon probably has the most developed strategy in the U.S. government, with a Cyber Command and thousands of people in different divisions of the military dedicated to matters of cybersecurity and cyberwafare.

The State Department's cyber coordinator, Christopher Painter, called cyber security a diplomatic priority for the United States as it seeks to defend itself from threats ranging from freelance hackers to militants to potential rival states.

"The most important thing is to build international consensus....It's not just China that we need to engage with. It is an important part of our agenda with every country," Painter told Reuters on the sidelines of a London conference.

(Additional reporting by Arshad Mohammed, Phil Stewart, Mark Hosenball, Sarah Lynch and Andrea Shalal-Esa in Washington and Peter Apps in London; Editing by Cynthia Osterman)

Can Google Know Where the gMail Attack Came From?

Friday, June 3, 2011

Can Google Know Where the Gmail Attack Came from?

The company blames China, but none of the evidence is definitive—which is the nature of such attacks.

By Erica Naone

On Tuesday, Google **revealed** a new spate of attacks aimed at Gmail users, and said the attacks appeared to have come from Jinan, China. The new attacks illustrate the difficulty of stopping hackers who use simple "social engineering" tricks to steal personal data, and they raise questions about how such attacks can ever be traced with certainty.

Personal accounts belonging to U.S. government officials, Chinese political activists, military personnel, and journalists were targeted, the company said in a blog post. Google has pointed to Chinese hackers before—in **early 2010** it said attackers from the country had stolen its intellectual property and tried to access the Gmail accounts of human rights activists. The Chinese foreign ministry has vigorously rejected the idea that the Chinese government was responsible for the attacks.

Google says the attackers did not exploit any security holes in the company's e-mail service. Instead, they involved tricking users into sharing their log-in information. Carefully tailored messages, apparently written by a friend or colleague, were used to direct victims to a fake log-in page where their details were captured. This technique, known as "spear phishing," was also used recently to steal information from the prominent security company RSA—information that may have been used to perform further attacks on the company's customers.

Experts say this type of attack is hard to stop; unlike other types of attacks, there is no technical fix. "I think of incidents like this more as a series of successes and failures on the part of the attacker," says Nart Villeneuve, a senior threat researcher at **Trend Micro**, which makes antivirus, antispam, and Internet security software. "It's more of a campaign than it is a single attack."

Before joining Trend Micro, Villeneuve was heavily involved in tracking attacks on human-rights activists—he was part of the group that revealed a complex hacking operation that spied on figures including the Dalai Lama.

Villeneuve also says it's hard to identify the real source of this type of attack in order to

Can Google Know Where the gMail Attack Came From?

cut it off. To pinpoint the source of the recent incidents, Google likely looked at a variety of clues, he says. The company could examine the IP addresses used to access e-mail accounts, which can reveal a user's location. The company could also look at the servers used to host fake log-in pages and collect users' personal information.

But this alone isn't enough, Villeneuve says. Attackers can easily take over computers located somewhere else, and use them to launch an attack. "Making your attack seem like it came from somewhere else is not hard," he says.

So Villeneuve says Google probably looked at many more clues to decide the source of the recent attacks. For example, he says, the company could have looked for patterns in the times that the attacks took place. Villeneuve believes that "from their point of good visibility, they could build up a lot of information."

Even then, Villeneuve emphasizes, it is extremely difficult to pin responsibility for the attacks on any single entity, organization, or nation.

Bruce Schneier, a prominent computer security expert and chief security officer of the British company BT, agrees. "Attacks don't come with a return address," he says. "This is a perennial problem. It's not a problem of anonymity; it's a problem of how the Internet works."

While there's good reason to suspect Chinese involvement, there's no way to know for sure, Schneier says. Routing an attack through China would be an excellent way for another interested party to throw investigators off their track, he says. But Schneier adds that the type of attack leveled at Gmail users is happening all the time.

Security researcher **Mila Parkour** identified and **posted samples** of some of the fake e-mail messages and fake Web pages used to trick Gmail users into handing over their log-in information. She notes that "the spear phishing method used in this attack is far from new or sophisticated," but points out that Web mail services offered by Google, Yahoo, and others don't offer users the same level of protection as many enterprise systems. What's more, she says, many users forward messages from business accounts to personal accounts, making the personal accounts worth targeting.

Villeneuve says that in some of the Web mail attacks he's studied, attackers seem to be gathering information about a user's computer or antivirus software. Since many people check personal e-mail at work, attackers might also be looking to gather information about systems at other locations that they want to target later, Villeneuve

Can Google Know Where the gMail Attack Came From?

believes.

Though Google has gained headlines for coming forward with the recent news, Villeneuve notes that targeted attacks aimed at high-value individuals are "not just a Google problem." He's recently identified similar examples aimed at users of Yahoo mail and Hotmail, but he cannot confirm that they are related.

Pinning Hacking Blame on China Could Be Tough: CNO

Pinning hacking blame on China could be tough: CNO

By [Andrea Shalal-Esa](#)

WASHINGTON | Thu Jun 2, 2011 6:28pm EDT

(Reuters) - Pinning the blame for a recent attack on the networks of Lockheed Martin Corp and other defense contractors on [China](#) could be difficult, the top U.S. naval officer said on Thursday

Chief of Naval Operations Admiral Gary Roughead said he had not been briefed on any finding by U.S. intelligence agencies that China was likely behind what Lockheed Martin Corp has described as a "tenacious" attack on its networks.

Experts and agencies looking into the May 21 incident have a growing suspicion that some individual or entity in China was responsible, although they note that clever hackers usually lay elaborate false trails to cover their tracks.

Roughead said it was challenging to reach definitive conclusions about where cyber attacks originated.

"Folks tend to tie a lot of the hacking activity to China, but ... my sense is that you're moving into a realm (where) you can't always say it's a state actor," Roughead told Reuters in an interview. "When people talk about attribution, I take it with a grain of salt."

Pointing to the computer on his desk, he said, "A non-state actor ... could attack somebody through my box here, and if you traced it back, you'd see it came from this office, when in point of fact, this was just a way point that somebody used."

Roughead's comment came a day after Google Inc said unknown hackers, likely from central China, tried to hack into the Gmail accounts of hundreds of users, including

Pinning Hacking Blame on China Could Be Tough: CNO

senior U.S. government officials.

Neither Google nor the U.S. government has said the Chinese government was behind the attacks. Google said only that the attack appeared to originate in China.

It was not immediately clear if there was any link between the Google and Lockheed attacks.

Roughead said technology issues tended to dominate public discussion about cybersecurity, but the bigger issues involved policy and regulatory responses.

Washington has said that the United States could respond to a devastating cyber attack with real-world military retaliation, but U.S. government officials say proving Beijing or other countries were responsible could be difficult.

In the end, tight security and financial sanctions or cyber countermeasures could prove to be a more powerful deterrent than military action, said one defense official, who was not authorized to speak publicly.

STRATEGY RELEASE POSTPONED

Deputy Defense Secretary William Lynn, Vice Chairman of the Joint Chiefs of Staff General James Cartwright, and General Keith Alexander, who heads U.S. Cyber Command, had planned to release a new Pentagon cyber strategy next week, but the rollout has been postponed until later this month while final details are being hammered out, two defense officials said.

The strategy will codify general principles laid out by Lynn in recent months in various speeches and an article in Foreign Affairs magazine published in October 2010, said one official, who was not authorized to speak on the record.

It will encourage international cooperation and establishment of norms and

Pinning Hacking Blame on China Could Be Tough: CNO

information-sharing standards to help regulate activity on global networks, the official said.

One model could be the system of compliance used by the Centers for Disease Control, said the official.

Roughead said the military was also looking at whether it should adopt a deterrence policy for cyberpolicy that mirrored the one used for nuclear weapons during the Cold War, but said no firm conclusions had been reached.

The Navy is trying to be proactive on the cyber front through creation of a separate cyber command, or Tenth Fleet, that was monitoring all Navy networks, and had created a new "Center for Cyber Security Studies" at the Naval Academy.

In addition, two courses were added to the curriculum there for non-cyber experts to help educate future Navy leaders about the risks and challenges of computer networks.

Lockheed officials said they were unaware of any new finding on who was behind the attack on its networks, repeating a statement issued last weekend, in which the company said it warded off the attack, taking aggressive actions to protect systems and data. No compromise of customer, program or employees' personal data had occurred, the company said.

(Reporting by Andrea Shalal-Esa, additional reporting by Mark Hosenball and [Phil Stewart](#) in Washington and [Karen Jacobs](#) in Atlanta, editing by Matthew Lewis)

Cyber Spies Target Chinese Experts

Cyberspies Target China Experts

By SIOBHAN GORMAN



Recent attempts to hack U.S. officials' Gmail accounts are part of a broad Chinese cyberspying scheme, but China's government denies any role. Meanwhile, Nintendo has its own security issues after it was hacked. Andrew LaVallee and Jake Lee discuss.

Chinese cyberspies, who targeted the personal Gmail accounts of top U.S. officials, are trying to gain access to computers belonging to China specialists and defense contractors who circulate in and out of government and talk regularly with those in power, according to security experts who have tracked these schemes.

The stealth infiltration campaign, similar in tactics to the Gmail scheme that Google Inc. disclosed last week, represents cyberspies' efforts to circumvent the high security walls on official government email accounts.

Such targeted "phishing" expeditions involved sending booby-trapped emails to people who have information a hacker is seeking. The emails typically appear to have been sent by a trusted colleague and ask the

Cyber Spies Target Chinese Experts

recipient to open an attachment. When that is done, a malicious software program is placed on the computer that could perform multiple functions, such as tracking all keystrokes or providing full access to an organization's computer network. They frequently are used to obtain access to passwords and private correspondence.

Their occurrence has spiked in the past few months, security experts say. Kevin Mandia, CEO of the security firm Mandiant, said his firm saw four to five times the average number of attacks from China in April. "It was a huge uptick," he said.

The attacks have been traced to China, but that doesn't necessarily mean they are directly ordered by the government. Spokesman Wang Baodong for the Chinese Embassy in Washington denied any government involvement in such cyberspying schemes. "As a responsible player in cyberspace, China strongly opposes unlawful online activities and supports international cooperation in striking down on such misdeeds," he said. "Any claims of so-called Chinese state support for hacking are completely fictitious, and blaming misdeeds on China is irresponsible and unacceptable."

Targeting people on the periphery of power is more likely to pay off because their computer systems are often less protected than the U.S. government, and these individuals frequently discuss sensitive issues with those in government. That was likely why the Google infiltrators targeted the personal emails of government officials.

"It's a routine occurrence now because think tanks are soft targets and you get good data," said James Lewis, a former State Department official and current cybersecurity specialist at the Center for Strategic and International Studies who has advised the Obama administration on cybersecurity policy. He said he was the target of a combined telephone and phishing attempt in 2010. "I just assume that all our communications are insecure."

Cyber Spies Target Chinese Experts

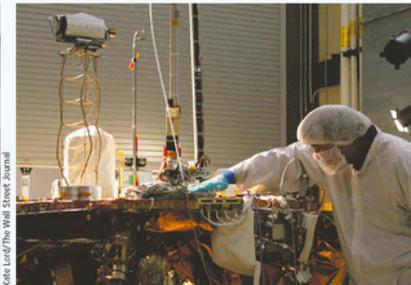
James Mulvenon, a China and cyber-security expert, has been tracking a four-year phishing campaign against China specialists in Washington. He's logged more than 100 rounds of attacks against 30-40 China specialists, many of whom have rotated in and out of government.

"I was struck by the breadth of it," he said. "They had targeted huge numbers of China specialists all over D.C.," both former government officials and those about to take federal jobs. "They want to find people who have access."

The goal of this campaign in Washington appears to be to gather information from individuals who communicate with U.S. officials about China matters, Mr. Mulvenon said. If cyberspies gather sensitive but unclassified data from Washington research institutions and a smattering of U.S. officials, he said, "you get a pretty good picture of what's going on in Washington as it relates to China."

The New Battleground

The New Battleground | Security officials say Chinese-related cyberattacks are on the rise.

<p>May 1999: The accidental U.S. bombing of the Chinese Embassy in Belgrade, Serbia, leads to a series of defacements of U.S. government Web sites by Chinese hackers.</p>	<p>April 2001: The collision of a U.S. Navy reconnaissance plane and a Chinese F-8 fighter sparks denial-of-service attacks and Web defacements against government and private sites.</p>	<p>November 2004: Chinese hackers reportedly attack unclassified U.S. military systems including the Defense Information Systems Agency, and the Army Space and Strategic Defense installation.</p>	<p>November 2006: Chinese hackers attack the U.S. Naval War College computer infrastructure, possibly targeting war-game information. The college's email system is down for at least two weeks.</p>	<p>October 2007: China is suspected as the source of a malicious email targeting 1,100 employees at the Oak Ridge National Lab, allowing access to a database at the nuclear-weapons laboratory.</p>	<p>March 2009: A Canadian study describes a Chinese network that targeted more than 1,300 hosts including those at the German, Indian, Pakistani and Portuguese embassies.</p>
					
<p>Google says it was targeted.</p>	<p>A Chinese fighter and a U.S. Navy plane (remains above) collided in 2001.</p>	<p>EMC's RSA tokens put at risk.</p>	<p>Lockheed Martin, builder of the Mars lander (above), says it was hacked.</p>		
<p>January 2010: Google says Chinese hackers breached its systems. Other companies attacked include Juniper Networks and Adobe Systems.</p>	<p>January 2010: Report from British intelligence issued in 2008 that warning companies about the threat from Chinese hacking becomes public.</p>	<p>February 2011: Computer security firm McAfee says in a report that it found evidence that Chinese hackers attacked five Western oil companies.</p>	<p>March 2011: EMC Corp.'s security division, RSA, says its systems were infiltrated using 'phishing' emails. Chinese hackers are strongly suspected for the attack.</p>	<p>May 2011: Defense contractor Lockheed Martin acknowledges its computer systems were hacked. Chinese hackers are reportedly suspected.</p>	<p>June 2011: Google says Chinese hackers targeted the email accounts of senior U.S. officials and hundreds of other prominent people.</p>

The campaign attempts to trick China specialists into opening attachments that would provide hackers access to their computers. In the beginning, Mr. Mulvenon said, the emails were easily identifiable as fraudulent. They

Cyber Spies Target Chinese Experts

contained lots of spelling errors and odd wording choices that would make more sense in Chinese than American English.

But the recent ones appear to come from people the target would know and contain text that plausibly could have been written by the alleged sender of the email, he said. The topics range from meeting agendas and the Olympics to President Barack Obama's trip to China and conference invitations.

One such email in November 2009 purported to come from Dennis Wilder, a former Asia specialist on the National Security Council in the George W. Bush administration who was at the Brookings Institution at the time.

The email discussed a recent press briefing by the Chinese ambassador on climate change, and it contained an attachment concealing a virus that claimed to be a transcript of the press briefing. Mr. Wilder hasn't owned a Gmail account.

Another well-crafted phishing scheme duped a group of defense contractors. In 2008, one Defense Department agency held a conference, and then posted some of the presentation materials online, including the names and email addresses of the 50 or so attendees.

Soon after, the attendees, mostly defense contractors, received emails that purported to be from one of the presenters at the conference and included an attachment that claimed to be his presentation materials, according to a person familiar with the incident.

A majority of the conference attendees opened the attachment, which downloaded on to their computer malware that provided "unfettered access" to their computer, this person said. "There was widespread success by the bad guys." A subsequent investigation tracked the perpetrator back to a Chinese hacking group.

"They're still doing the exact same thing" today, the person familiar with the

Cyber Spies Target Chinese Experts

incident said of the hacking group.

China Linked to New Breaches Tied to RSA

JUNE 6, 2011 4:00 AM PDT

China linked to new breaches tied to RSA

by [Elinor Mills](#)

Recent attacks on three U.S. defense contractors could be tied to cyberespionage campaigns waged from China, several security experts told CNET.

[The incidents](#) at Lockheed Martin, L-3 Communications, and Northrop Grumman appear to stem from a breach at RSA [in March](#) in which data was stolen related to RSA's SecurID two-factor authentication devices--widely used by U.S. government agencies, contractors, and banks to secure remote access to sensitive networks.



Lockheed confirmed to [The New York Times](#) on Friday that hackers had used data stolen in the RSA breach and other methods to figure out the coded password of a Lockheed contractor, but that Lockheed had blocked the attack before any sensitive data could be exposed. The company said it was replacing 45,000 SecurID tokens.

L-3 told employees in April that it was targeted using information acquired from the RSA breach, [Wired reported](#). And Northrop Grumman, meanwhile, unexpectedly shut down remote access to its network last month, leading to speculation that there had been a SecurID-related incident, according to [FoxNews.com](#).

When RSA warned customers that their SecurID deployments could be affected by the intrusion, the industry was waiting for the proverbial other shoe to drop. Thus, word of the defense contractor attacks came as no surprise. And the timing is such that it seems unlikely to be coincidental, the experts said.

Two-and-a-half months is plenty of time for whoever stole the data to sell it to interested parties in underground channels and for buyers to prepare attacks that take advantage of the pilfered information--basically figuring out which key on the key chain goes to which door. But it's also a small enough window of time to let those attackers catch some RSA customers before they can change the locks.

Having the key, or token, isn't enough to break into a system. Attackers also need to

China Linked to New Breaches Tied to RSA

have the passcode that token holders use when they are logging in to a network. Phishing e-mails that trick recipients into revealing their log-ins and e-mails bearing malware that infects the recipient's computer are commonly used to get that information. Having done their homework, the attackers know to craft an official-looking e-mail coming from a person or organization the recipient would trust.

Such sophisticated attacks on a specific target that are designed to steal credentials in order to get into the network to access critical data are known as Advanced Persistent Threats, or APT.

The RSA breach was accomplished using an APT, and [Google cited APT in early 2010](#) as the method used in an attack on its network in which intellectual property was stolen. Google specifically said the attack originated in China and that Gmail accounts of human rights activists in the U.S., China, and Europe were separately compromised. Yahoo, Symantec, Northrop Grumman, and Dow Chemical were reportedly among the 30 or so other targets.

"APT is a euphemism for China," said Rich Mogull, chief executive of Securosis. "There is a massive espionage campaign being waged by a country. It's been going on for years, and it's going to continue."

Chinese representatives in the U.S. could not be reached for comment Friday, but government officials denied any involvement in the Google attacks last year. They also denied any responsibility in phishing attacks targeting Gmail accounts of officials in the U.S. and Asian countries, political activists, and journalists that Google [announced last week](#). In fact, a Chinese official turned the tables and accused the U.S. of launching an Internet war against other countries, according to [The Associated Press](#).

Meanwhile, the [Pentagon is now saying](#) it plans to issue new strategy declaring that in certain circumstances it will view cyberattacks from foreign nations as an act of war meriting military response.

"The reality is, part of the basis of U.S. hegemony...has been the ability to leverage command of signals intelligence to have perspective on the motivations and activities of others. Cyberspace has equalized that, so all of a sudden we're in a competitive intelligence environment," said Rafal Rohozinski, a principal at SecDev who did research on targeted attacks on Tibet and others with supposed links to China. Those attacks were detailed in a "GhostNet" report [in 2009](#).

Espionage is common among the major nations, but reports of cyberespionage from China have increased over the past decade, campaigns that are ostensibly focused on silencing dissidents and other detractors, or reducing China's technology gap with the U.S. and other major countries.

"China has made no secret that they see cyberspace as the domain that allows them to compete with the U.S.," Rohozinski said.

China Linked to New Breaches Tied to RSA

It's easy to connect the dots between the various attacks, particularly considering what the motivation may be behind them. However, there is often no way to know for sure where a cyber attack originated because attackers can easily hide their tracks.

"I think [the attacks on the contactors] are completely related" to the RSA intrusion, said Chris Wysopal, chief technology officer at Veracode. "While I think they're related, I don't necessarily think it is the same group" that's responsible.

Just like in the financially motivated credit card criminal underground, there is an ecosystem around information that can be used for corporate or government cyberespionage, according to Wysopal. "The RSA attackers knew that what they were stealing could be sold to lots of governments," he said.

"If it's any kind of military espionage, military adversaries are going to be high on the list," Wysopal said. "The question then is who in China--is it government agents or independent contractors selling to the Chinese government?"

Security 'Tokens' Take Hit

Security 'Tokens' Take Hit

RSA Offers to Replace Nearly All of Its SecurIDs in Use or Provide Monitoring

By [SIOBHAN GORMAN](#) And [SHARA TIBKEN](#)

RSA Security is offering to provide security monitoring or replace its well-known SecurID tokens—devices used by millions of corporate workers to securely log on to their computers—"for virtually every customer we have," the company's Chairman Art Coviello said in an interview.

[View Full Image](#)



Joe Schram/The Wall Street Journal

RSA SecurID

In a letter to customers Monday, the [EMC Corp.](#) unit openly acknowledged for the first time that intruders had breached its security systems at defense contractor [Lockheed Martin Corp.](#) using data stolen from RSA.

SecurID tokens have become a fixture of office life at thousands of corporations, used when employees log onto computers or sensitive software systems. The token is an essential piece of security, acting as an ever-changing password that flashes a series of six digits that should be virtually impossible to duplicate.

Mr. Coviello didn't specify what happened to the tokens at Lockheed. The intruders didn't take any Lockheed customer or employee data. But as a

Security 'Tokens' Take Hit

precaution, he said RSA will offer to replace nearly all tokens—millions of them used by government agencies and businesses ranging from Rolls Royce Motor Cars Ltd. to PokerStars.com.

Some customers may not need to replace them because of their specific security needs, he said. "We believe and still believe that the customers are protected."

Mr. Coviello said RSA will provide transaction monitoring and other detection capabilities for customers, particularly for financial institutions.

In March EMC disclosed it had been hit by a sophisticated cyberattack on its SecurID products. It advised customers to beef up their own security, such as making sure no rogue programs had been installed on servers running RSA software. It also suggested users increase the length of employee "PIN" numbers used in tandem with the digits spit out by the RSA token.

As the company did a forensic analysis of the attack, it began to suspect the attacker was focused on defense contractors based on the sophistication of the attack and the profile of the hacker.

"Their modus operandi led us to believe this perpetrator was likely to attack defense secrets and related intellectual property," Mr. Coviello said, of the intruders. The Lockheed infiltration received high-level attention in Washington, including from President Barack Obama, who was briefed on the incident.

Shortly after concluding defense customers were likely targets, RSA began working with its government and military-contractor customers, and offered to replace all their SecurID tokens, which Mr. Coviello said was key to preventing further attacks.

Some analysts said RSA's token replacement program is a smart move but

Security 'Tokens' Take Hit

that the breach will still hurt its reputation.

"It would have been better if RSA was more forthright from the beginning. They unnecessarily damaged their reputation by holding back," said Gartner analyst Mark Diodati.

Mr. Coviello said his company has provided the right amount of information to its customers. Providing any further information, he said, would give the hackers a blueprint for how to mount further attacks.

Companies have been hit by a wide range of attacks in recent weeks. Sony Corp., PBS and users of Google Inc.'s Gmail are among recent examples. The RSA incident raised the most alarms given the company's core competence—computer security—and the central role it plays in guarding the systems of major U.S. corporations.

Lockheed became the first confirmed breach related to the RSA issue, with the U.S. weapons manufacturer saying an investigation into last month's cyber attack on the company "concluded that the RSA breach was a direct contributing factor."

"RSA has been with us every step of the way since our breach, and we're replacing all of our SecurID tokens," Lockheed spokeswoman Jennifer Whitlow said. "They did review our investigation details and have offered to help out as they could."

The Lockheed attack showed that it was technologically feasible to hack a third-party using data taken from RSA, and the defense contractor may not be the last example. Mr. Coviello said that "I'm not suggesting we won't see some other attacks in the interim given the scale of the Lockheed attack, but it is the only confirmed attack we have using the [stolen] information."

He added that RSA is working with other companies rumored to have experienced attacks due to the RSA breach, but declined to identify the

Security 'Tokens' Take Hit

customers.

"Because of these attacks and the changing threat landscape there has been and incredible heightening of public awareness," Mr. Coviello said.

"The whole thing has reached a crescendo where customers don't want to tolerate any level of risk, whether it's real or perceived."

RSA to Replace SecurID Tokens Following Breaches

JUNE 7, 2011 6:04 AM PDT

RSA to replace SecurID tokens following breaches

by [Lance Whitney](#)

Following recent cyberattacks against several defense contractors, in which hackers breached security using stolen SecurID keys, SecurID maker RSA is promising to replace the tokens for customers concerned about the vulnerability of their network data.

In an [open letter to all SecurID customers](#), RSA Executive Chairman Art Coviello acknowledged that the likely motive behind the March theft of SecurID token information was to obtain defense secrets and related intellectual property. RSA specifically [warned customers](#) at the time that the theft could breach their security.

In late May, defense contractor [Lockheed Martin revealed](#) that it had been attacked by intruders who had created duplicates of the stolen SecurID keys. Incidents also occurred at L-3 Communications and Northrop Grumman. Security experts have told CNET that the attacks could be tied to [cyberespionage campaigns waged from China](#).

A SecurID token generates a constantly changing series of numbers that employees of a company can use in combination with their own passwords to access their corporate networks.

Though unrelated to the SecurID incident, a wave of cyberattacks have recently hit other companies, including [Epsilon](#), [Sony](#), [Google](#), [PBS](#), and [Nintendo](#), which Coviello said "point to a changing threat landscape and have heightened public awareness and customer concern."

In an effort to calm customers worried about their own security, Coviello said that although he remains confident in SecurID as an authentication system, RSA will expand its security efforts in two key ways:

- It will replace the SecurID tokens for customers that need to protect their intellectual property and corporate networks, which in essence could apply to all of the company's customers.
- It is offering to set up specific "risk-based authentication strategies" for customers with a large number of users who typically conduct online financial transactions.

Coviello is promising to work with customers to review their risk levels and user base to determine which option would be most effective and yet the least disruptive to their operations.

Beyond these measures, Coviello said that the company plans to continue to invest in

RSA to Replace SecurID Tokens Following Breaches

its SecurID technology in an attempt to strengthen its authentication and its ability to detect "suspicious behavior targeted at networks, transactions and user sessions."

US Military, Businesses Seek Better Defenses on the Inside

Wednesday, June 8, 2011

U.S. Military, Businesses Seek Better Defenses on the Inside

Research projects at the Pentagon highlight the need to prevent data theft that happens within an organization's walls.

By Robert Lemos

For most of the history of the Internet, companies and government agencies have split networks into two categories: internal, trusted systems and external, untrusted ones. The most common approach to security has been to erect a wall that treats data and communications as potentially dangerous if they come from outside and safe if they come from within.

Yet some of the most serious breaches, such as the massive handover of U.S. State Department cables to WikiLeaks late last year, come from corporate and government insiders. Even if they mean no harm, insiders can present security risks: several major data breaches have occurred after attackers tricked employees into downloading malicious software that took hold inside the organization's firewall.

"In the early 2000s, you would see a lot of organizations focus on outsiders exclusively," says Joji Montelibano, who leads the insider-threat technical team at the Software Engineering Institute's CERT program at Carnegie Mellon University. "With the prevalence of information technology everywhere now, the ways an insider can harm an organization have increased dramatically."

In hopes of counteracting the trend, the Defense Advanced Research Projects Agency (DARPA)—the research arm of the U.S. military—has called for research that would improve the government's ability to identify threats from within. DARPA is taking a two-pronged approach: last August, an agency project named Cyber Insider Threat (CINDER) called for proposals for better systems to detect attackers who have already compromised a network. Two months later, DARPA launched Anomaly Detection at Multiple Scales (ADAMS), to detect insiders just before or after they go rogue.

The proposed ADAMS technology will likely model typical user behavior and alert managers when a user is acting off-profile. Such a system, for example, could have caught Bradley Manning, the U.S. intelligence analyst who is alleged to have leaked the diplomatic cables, by warning officials that Manning had suddenly accessed

US Military, Businesses Seek Better Defenses on the Inside

thousands of cables from his computer.

"If I'm trying to get information out of my company, I'm probably going to start at the simplest level and work my way up—I would try to e-mail it to myself, I would try to post it to a website, or upload the file to a peer-to-peer network," says Daniel Guido, a consultant with iSec Partners, who frequently tests firms' security to identify potential weaknesses. "They are going to approach exfiltrating information outside the company in a very particular way, and if you think like they do, you will be much more effective" as a defender.

The problem is difficult, though, if the systems attempt to take in many variables, says Malek ben Salem, a graduate student and computer-science researcher at Columbia University. She has been trying to model search behavior in order to detect when an attacker is going beyond the normal scope of his job or impersonating someone with legitimate access. Because attackers might not know a file system or other aspects of corporate network as well as a legitimate employee does, they tend to search more extensively. In experiments, Ben Salem says her model has detected 100 percent of masqueraders with a rate of false positives of only 1 percent.

The CINDER project looks for activity in a system that suggests of an attack launched from the inside. For instance, a worm like Stuxnet, which is believed to have damaged Iran's nuclear program, could be detected by looking for the changes it has made to system files and network disks.

"CINDER will attempt to address some of the flaws in current detection systems by modeling the adversary mission—not by attempting to monitor a person or their particular traits—and by beginning with the assumption that a given system has already been compromised," Peiter "Mudge" Zatkó, the manager in charge of the program at DARPA, said when the project was announced.

Increasingly, companies that sell security products are adding features that may help detect insider attacks. For example, firewalls and other security systems have been fortified with software that scans for encrypted e-mail. Some security companies advocate deploying decoy files that no employee should ever access, and alerting managers when they are accessed. Coupling decoy files with current research into modeling legitimate user behavior could detect a wide variety of attacks, says Columbia's Ben Salem.

However, insider attacks cannot be thwarted by just creating a better network appliance, says SEI CERT's Montelibano. Better policies and security measures are

US Military, Businesses Seek Better Defenses on the Inside

important as well, such as allowing only approved applications to be run inside a network and limiting e-mail attachments.

"The big finding of our research is that insider threats are not just a technical problem," he says. "What we still see is organizations throwing technology at the problem. But our research reveals that by and large, insiders' technical activity is preceded by observable behavioral activity."

Anonymous Warns NATO Not to Challenge It

JUNE 9, 2011 9:26 AM PDT

Anonymous warns NATO not to challenge it

by [Lance Whitney](#)

Responding to a recent report from the North Atlantic Treaty Organization condemning Anonymous, the online "hactivist" group has issued a public response warning the global organization not to challenge it.

Claiming that the NATO report singled it out as a threat to "government and the people," Anonymous defended some of its recent actions in the name of freedom and dissent. In [its message \(Google cached version\)](#), it also asserted that NATO fears the group not because it's a "threat to society," but because it's a "threat to the established hierarchy."

Issued last month by Lord Joplin, general rapporteur of NATO, [the report](#) warned member nations about the rising threat of "hactivism," or carrying out cyberattacks for political purposes. Singling out Anonymous, NATO described several of the group's most recent actions, including the [distributed denial-of-service attacks](#) against MasterCard, Visa, PayPal, Amazon, and others that had cut off services for WikiLeaks.

Noting that Anonymous has become more sophisticated, the NATO report cautioned that it could hack into sensitive government, military, and corporate information and described a strong response against the group.

"Today, the ad hoc international group of hackers and activists is said to have thousands of operatives and has no set rules or membership," said the report. "It remains to be seen how much time Anonymous has for pursuing such paths. The longer these attacks persist the more likely countermeasures will be developed, implemented, the groups will be infiltrated and perpetrators persecuted."

In its response, Anonymous tried to soften its stance in parts by saying that it doesn't want to threaten anyone's way of life or terrorize any nation. But it made clear its reaction to NATO's report.

"Finally, do not make the mistake of challenging Anonymous," warned Anonymous in its message. "Do not make the mistake of believing you can behead a headless snake. If you slice off one head of Hydra, ten more heads will grow in its place. If you cut down one Anon, ten more will join us purely out of anger at your trampling of dissent."

NATO's report also provided a larger look into the growing danger of cyberattacks and how governments should respond to them. In the report, Joplin asked the question of how NATO should react if one of its member nations was the victim of a cyberattack.

Anonymous Warns NATO Not to Challenge It

"Can one invoke [Article 5 of the Washington Treaty](#) after a cyber attack?" asked the report. "And what response mechanisms should the Alliance employ against the attacker? Should the retaliation be limited to cyber means only, or should conventional military strikes also be considered?"

Both the U.S. and the U.K. have recently [made their own positions clear](#)--that they consider cyberwarfare another form of warfare, and one potentially subject to a response using conventional military weapons.

Anonymous Message to NATO

An Anonymous Message to NATO

Greetings, Members of NATO.
We are Anonymous.

In a recent publication, you have singled out Anonymous as a threat to "government and the people". You have also alleged that secrecy is a "necessary evil" and that transparency is not always the right way forward.

Anonymous would like to remind you that the government and the people are, contrary to the supposed foundations of "democracy", distinct entities with often conflicting goals and desires. It is Anonymous' position that when there is a conflict of interest between the government and the people, it is the people's will which must take priority. The only threat transparency poses to government is to threaten government's ability to act in a manner which the people would disagree with, without having to face democratic consequences and accountability for such behaviour. Your own report cites a perfect example of this, the Anonymous attack on HBGary.

Anonymous has issued a response to a recent NATO report, warning NATO not to challenge it.

(Credit: Screenshot by CNET)



Navy Rolls Out Regional Cybersecurity Centers

Navy Rolls Out Regional Cybersecurity Centers

Globally deployed network centers to function under Navy Fleet Cyber Command

(DEFENSE SYSTEMS 09 JUN 11) ... Amber Corrin

The Navy is preparing to launch initial operations at four new regional network operation security components that will support the Navy Fleet Cyber Command and help protect naval computer networks, one top Navy official said June 9.

“These [commands] 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.

The regional components are estimated to reach initial operating capability around July 1, with full operational capability expected in roughly 18 months, Deets said at the AFCEA Naval IT Day in Vienna, Va.

“It’s critical we take the best of the best and apply it across the world,” he said.

The regional components will be part of Navy efforts to tackle the broader network challenges Deets outlined in his comments, including a complex networking environment that comprises 750,000 users and thousands of networks, servers and devices.

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 cut nearly 1,000 networks, 20,000 servers and more than 32,000 devices, Deets said.

“The fewer number of networks we’re attempting to secure out there, the better,” he said. “We’ve tremendously reduced our vulnerability.”

Deets also said the Navy must improve its ability to define the risks it faces – and how to tackle those risks.

“We’re good at understanding risk and the willingness to mitigate it; we’re good at articulating that there is a risk. But we’re not good at articulating how big of a risk there is, or how much needs to be done to mitigate it,” Deets said. “We have to be able to calculate real risk. Is there risk in social media or instant messaging? How do we get our arms around that?”

But he acknowledged that not every risk can be mitigated and there must be some level of risk acceptance, such as the Navy’s decision to use social networking despite the possible risks it could pose.

Citi Data Theft Points Up a Nagging Problem

June 9, 2011

Citi Data Theft Points Up a Nagging Problem

By **ERIC DASH**

Citigroup's revelation that hackers stole personal information from more than 200,000 credit card holders makes it one of the largest direct attacks on a major bank.

Even more striking is that similar data breaches have been occurring for years — and the financial industry has failed to prevent them.

Details remain scarce, but the disclosure of the Citigroup breach on Thursday quickly turned into a debate on whether the banks and major credit card companies had invested enough money to safeguard the personal information of their customers.

“They’re not at all on top of it,” said Avivah Litan, a financial security analyst at Gartner Inc. “It’s almost shocking.”

In Washington, the finger-pointing has already begun. Sheila C. Bair, the chairwoman of the Federal Deposit Insurance Corporation, said on Thursday that she planned to call on some banks to strengthen their authentication procedures when customers log onto online accounts. That’s on top of new data security rules that federal regulators are completing.

Lawmakers, meanwhile, said they were outraged that Citigroup waited since early May to notify its customers; some are preparing legislation.

Representative James R. Langevin, a Rhode Island Democrat, said he was “shocked and disappointed” to learn of Citi’s delayed disclosure. “They knew the customers’ data was

Citi Data Theft Points Up a Nagging Problem

potentially exposed in May and only now are they telling them about the threat,” he said. “Being more forthcoming is essential.”

Consumers, meanwhile, are feeling increasingly vulnerable amid recent reports of data breaches at big companies, like Lockheed Martin, Epsilon and Sony.

A. J. Angus, a 25-year-old Google employee, was put in double jeopardy. On Thursday, he learned that his Citi credit card data had been stolen. Only a few weeks earlier, he learned that personal data on his [Sony PlayStation 3](#) was compromised.

“You have to be vigilant,” he said, adding that he periodically checks his credit report and looks over his transactions almost daily on a personal finance Web site.

On Thursday, Citigroup began notifying about half of the 200,000 affected customers that it planned to replace their credit cards after it discovered last month that hackers had gained access to its computer systems. The bank said that the thieves obtained customer names, card numbers, addresses, and e-mail details.

Social security numbers, expiration dates and the three-digit code found on the back of most credit cards were not compromised — a move that security experts say makes the exposed cardholders less likely to become fraud victims.

Neither Citigroup’s debit card business nor its online banking operations were breached.

“Citi has implemented enhanced procedures to prevent a recurrence of this type of event,” the company said in a statement.

Citi Data Theft Points Up a Nagging Problem

The intrusion is not all that unique. Over the last six years, there have been 288 publicly disclosed breaches at financial services companies that exposed at least 83 million customer records, according to the Identity Theft Resource Center.

Credit card industry officials say security issues go to the heart of their brands and they are trying to keep up with ever-more sophisticated criminals.

“We’re not dealing with 14-year-old hacker kids,” said Steve Elefant, the chief information officer at Heartland Payment Systems, which overhauled its security measures after the systems it used to process credit and debit card transactions were hacked in 2008. “We’re talking about 21st-century bank robbers — sophisticated, organized criminal gangs, located mostly in Eastern Europe and the U.S.”

Making matters worse, nearly every step along the payment chain is outsourced from the time a card is swiped to the time a monthly statement arrives, leaving plenty of openings for enterprising thieves. Security is further hampered by a patchwork of data protection laws and regulatory agencies, each with limited mandates.

“We need a uniform national standard for data security and data breach notification,” said Representative Mary Bono Mack, a California Republican who is pushing for legislation on better consumer safeguards. “In the meantime, regulators need to do a better job of being a consumer watchdog.”

Big credit card lenders are loath to acknowledge another reason that the breaches keep happening: they are in the business of reducing the financial losses stemming from fraud, not preventing data theft in the first place. As a result, analysts say, they have devoted the bulk of their resources to trying to stop fraudulent transactions from

Citi Data Theft Points Up a Nagging Problem

occurring.

“Data breaches are one thing,” noted David Robertson, the publisher of The Nilson Report, a payments industry newsletter. “Acting on that information is another, and the systems in place to catch fraud when it is trying to be perpetrated are extremely good.”

Indeed, while the thieves have gotten more skilled, the amount of money the banks have lost to fraud has actually stayed the same over the last six years — and has sharply fallen since the early 1990s. Today, fraud costs the banks about 5 cents for every \$100 that is charged, compared with 15 cents for every \$100 in 1992, according to Nilson data.

Merchant advocates, meanwhile, say the banks have little incentive to reduce it more because, in some cases, it can be a source of income. Not only do they take in hefty charge-back fees from merchants — sometimes \$25 or more for each fraudulent purchase — but in many cases retailers must swallow the cost of the item fraudulently purchased.

Preventing data theft from occurring seems to be a lower priority. After the huge credit card data breach of a payment processor in 2005, the major credit card companies banded together to form a set of security standards for the industry. But six years on, compliance with those rules has been mixed. Although virtually all of the 1,000 biggest merchants meet those requirements, far fewer than 60 percent of the millions of mom-and-pop retailers and online merchants do, according to Visa data.

Other proactive steps have also fallen by the wayside because of their cost. In Europe and Asia, most credit and debit card issuers have switched to cards that use small chips embedded inside the plastic that do a better job protecting transaction data. In the

Citi Data Theft Points Up a Nagging Problem

United States, the banks and card companies have not adopted the technology, reasoning that retailers are unwilling to spend heavily to upgrade their existing card readers.

Likewise, some security experts say encrypting data as it flows across the entire payment network would make data far less vulnerable to being extracted by thieves. However, only a tiny fraction of merchants and processors have upgraded their systems.

Mr. Elefant said the industry needed to adopt the encryption technology more quickly. “Unfortunately, some companies look at breaches as the cost of doing business,” he said. “That’s not the right way to look at it. You need to be as secure as you possibly can be.”

Others suggest the banks need to do more to enlist their customers, like providing more regular fraud alerts and giving them more control to turn on and off their credit cards.

“What they don’t do enough of is engage the identity holder in the war against fraud,” said James Van Dyke of Javelin Strategy and Research, a payments consulting firm. “They greatly prefer to wage this battle solo.”

Tara Siegel Bernard, Riva Richmond and Nelson D. Schwartz contributed reporting.

Few Cyberattacks Are Cause for Major Retaliation

Experts: Few cyberattacks are cause for major retaliation

Attacks on government and private networks happen all the time and require subdued responses, some experts say

By [Grant Gross](#), IDG News Service
June 08, 2011 05:11 PM ET

Cyberattacks on U.S. networks by other nations may not always demand the same level of retaliation, and only attacks that cause major damage or loss of life should prompt similar responses, a group of national security experts said Wednesday.

Cyberattacks on private companies and even on the U.S. Department of Defense's network are commonplace and part of a long history of international espionage that the U.S. and other countries have engaged in for years, said some panelists speaking at a cyberwar discussion at the Center for Strategic and International Studies (CSIS) in Washington, D.C.

Presented with a scenario similar to a [computer compromise at RSA Security](#), in which the attackers also targeted defense contractor Lockheed Martin, defense consultant Franklin Miller said people getting upset with the attack seem to assume that the U.S. doesn't engage in some of the same practices.

"This is going to happen," said Miller, former senior director for defense policy and arms control at the U.S. National Security Council. "This is what intelligence organizations do."

CSIS fellow Adriane Lapointe presented Miller and other panelists with a series of reality-based scenarios and asked them what the appropriate U.S. government response should be. The CSIS panel came just days after the U.S. Department of Defense said it was [prepared to use force](#) to respond to some cyberattacks.

In some cases, attacks that appear to be sponsored by another nation -- including attacks that [Google blamed on China in early 2010](#) -- may prompt the U.S. to file formal complaints, the panelists said. In other cases, the U.S. may want to signal another country that it considered an attack unfair, although it may be more difficult for other countries to read cybersignals than to interpret military aircraft flying near their borders, said James Lewis, director of the CSIS Technology and Public Policy Program.

The cybersignals of displeasure can be clear, said Robert Giesler, former director of information operations and strategic studies in the DOD's Office of the Secretary of Defense. "There are ways

Few Cyberattacks Are Cause for Major Retaliation

you can noisily go about penetrating networks," he said.

In some cases, the signal may not be cyber in nature, Miller added. "You don't have to [signal] in the same medium," he said. "If you want to inflict pain ... you need to find the point of pain. It may not be in the cyberworld. It may be elsewhere."

Countries may need to negotiate rules of engagement for cyber-espionage, panelists said.

Part of the problem with retaliating against other nations for a cyberattack is that it's still difficult to pinpoint where an attack came from, Giesler said. In some cases, compromised companies may attribute an attack to another nation when it's really a case of industrial espionage, he said. In other cases, attacks may come from so-called "patriotic" hackers who are acting on their own initiative, he said.

Even in attacks on DOD networks, "attribution still remains foggy," Giesler said.

Asked about attacks on DOD networks by another country, the panelists said the U.S. should respond, but in most cases, in a limited way. Only if major damage was done should the U.S. consider responding with force, said Judith Miller, former general counsel at the DOD.

"You're not going to start a war over something like this," added Robert Deitz, former senior counselor to the director of the U.S. Central Intelligence Agency.

The response would change in the case of an attack causing major damage or killing U.S. residents, the panelists said. An attack that takes down a large portion of the U.S. electric grid or the banking system would likely require significant retaliation, Franklin Miller said.

Recent news reports have suggested that [China and Russia have probed the U.S. electric grid](#) for weaknesses. Panelists suggested that attacking the grid was a step up from probing it.

"This is the kind of message that needs to be put out by the United States government publicly, that inference with the grid constitutes an extremely serious act ... which would be subject to very serious retaliation," Franklin Miller said. "If you lose the ability to generate or distribute power to an entire region of this country, we are going to be in very serious trouble as a country."

Grant Gross covers technology and telecom policy in the U.S. government for The IDG News Service. Follow Grant on Twitter at GrantGross. Grant's e-mail address is grant_gross@idg.com.

Cyber Combat: Act of War

Cyber Combat: Act of War

Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force

By [SIOBHAN GORMAN](#) And [JULIAN E. BARNES](#)

WASHINGTON—The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force.

The Pentagon's first formal cyber strategy, unclassified portions of which are expected to become public next month, represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military.

In part, the Pentagon intends its plan as a warning to potential adversaries of the consequences of attacking the U.S. in this way. "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," said a military official.

[View Full Image](#)



Reuters

Cyber Combat: Act of War

The Pentagon is studying when cyber attacks justify military action. An Air Force security center in Colorado.

Recent attacks on the Pentagon's own systems—as well as the sabotaging of Iran's nuclear program via the Stuxnet computer worm—have given new urgency to U.S. efforts to develop a more formalized approach to cyber attacks. A key moment occurred in 2008, when at least one U.S. military computer system was penetrated. This weekend Lockheed Martin, a major military contractor, acknowledged that it had been the victim of an infiltration, while playing down its impact.

The report will also spark a debate over a range of sensitive issues the Pentagon left unaddressed, including whether the U.S. can ever be certain about an attack's origin, and how to define when computer sabotage is serious enough to constitute an act of war. These questions have already been a topic of dispute within the military.

One idea gaining momentum at the Pentagon is the notion of "equivalence." If a cyber attack produces the death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for a "use of force" consideration, which could merit retaliation.

The War on Cyber Attacks

Attacks of varying severity have rattled nations in recent years.

June 2009: First version of Stuxnet virus starts spreading, eventually sabotaging Iran's nuclear program. Some experts suspect it was an Israeli attempt, possibly with American help.

November 2008: A computer virus believed to have originated in Russia succeeds in penetrating at least one classified U.S. military computer network.

August 2008: Online attack on websites of Georgian government agencies and financial institutions at start of brief war between Russia and Georgia.

May 2007: Attack on Estonian banking and government websites occurs that is similar to the later one in Georgia but has greater impact because Estonia is more dependent on online banking.

The Pentagon's document runs about 30 pages in its classified version and 12 pages in the unclassified one. It concludes that the Laws of Armed Conflict—derived from various treaties and customs that, over the years,

Cyber Combat: Act of War

have come to guide the conduct of war and proportionality of response—apply in cyberspace as in traditional warfare, according to three defense officials who have read the document. The document goes on to describe the Defense Department's dependence on information technology and why it must forge partnerships with other nations and private industry to protect infrastructure.

The strategy will also state the importance of synchronizing U.S. cyber-war doctrine with that of its allies, and will set out principles for new security policies. The North Atlantic Treaty Organization took an initial step last year when it decided that, in the event of a cyber attack on an ally, it would convene a group to "consult together" on the attacks, but they wouldn't be required to help each other respond. The group hasn't yet met to confer on a cyber incident.

Pentagon officials believe the most-sophisticated computer attacks require the resources of a government. For instance, the weapons used in a major technological assault, such as taking down a power grid, would likely have been developed with state support, Pentagon officials say.

The move to formalize the Pentagon's thinking was borne of the military's realization the U.S. has been slow to build up defenses against these kinds of attacks, even as civilian and military infrastructure has grown more dependent on the Internet. The military established a new command last year, headed by the director of the National Security Agency, to consolidate military network security and attack efforts.

The Pentagon itself was rattled by the 2008 attack, a breach significant enough that the Chairman of the Joint Chiefs briefed then-President George W. Bush. At the time, Pentagon officials said they believed the attack originated in Russia, although didn't say whether they believed the attacks were connected to the government. Russia has denied involvement.

Cyber Combat: Act of War

The Rules of Armed Conflict that guide traditional wars are derived from a series of international treaties, such as the Geneva Conventions, as well as practices that the U.S. and other nations consider customary international law. But cyber warfare isn't covered by existing treaties. So military officials say they want to seek a consensus among allies about how to proceed.

"Act of war" is a political phrase, not a legal term, said Charles Dunlap, a retired Air Force Major General and professor at Duke University law school. Gen. Dunlap argues cyber attacks that have a violent effect are the legal equivalent of armed attacks, or what the military calls a "use of force."

"A cyber attack is governed by basically the same rules as any other kind of attack if the effects of it are essentially the same," Gen. Dunlap said Monday. The U.S. would need to show that the cyber weapon used had an effect that was the equivalent of a conventional attack.

James Lewis, a computer-security specialist at the Center for Strategic and International Studies who has advised the Obama administration, said Pentagon officials are currently figuring out what kind of cyber attack would constitute a use of force. Many military planners believe the trigger for retaliation should be the amount of damage—actual or attempted—caused by the attack.

For instance, if computer sabotage shut down as much commerce as would a naval blockade, it could be considered an act of war that justifies retaliation, Mr. Lewis said. Gauges would include "death, damage, destruction or a high level of disruption" he said.

Culpability, military planners argue in internal Pentagon debates, depends on the degree to which the attack, or the weapons themselves, can be linked to a foreign government. That's a tricky prospect at the best of times.

The brief 2008 war between Russia and Georgia included a cyber attack that disrupted the websites of Georgian government agencies and financial

Cyber Combat: Act of War

institutions. The damage wasn't permanent but did disrupt communication early in the war.

A subsequent NATO study said it was too hard to apply the laws of armed conflict to that cyber attack because both the perpetrator and impact were unclear. At the time, Georgia blamed its neighbor, Russia, which denied any involvement.

Much also remains unknown about one of the best-known cyber weapons, the Stuxnet computer virus that sabotaged some of Iran's nuclear centrifuges. While some experts suspect it was an Israeli attack, because of coding characteristics, possibly with American assistance, that hasn't been proven. Iran was the location of only 60% of the infections, according to a study by the computer security firm Symantec. Other locations included Indonesia, India, Pakistan and the U.S.

Officials from Israel and the U.S. have declined to comment on the allegations.

Defense officials refuse to discuss potential cyber adversaries, although military and intelligence officials say they have identified previous attacks originating in Russia and China. A 2009 government-sponsored report from the U.S.-China Economic and Security Review Commission said that China's People's Liberation Army has its own computer warriors, the equivalent of the American National Security Agency.

That's why military planners believe the best way to deter major attacks is to hold countries that build cyber weapons responsible for their use. A parallel, outside experts say, is the George W. Bush administration's policy of holding foreign governments accountable for harboring terrorist organizations, a policy that led to the U.S. military campaign to oust the Taliban from power in Afghanistan.

UK Developing Cyber-Weapons Programme to Counter Cyber War Threat

UK developing cyber-weapons programme to counter cyber war threat

Military to gain a new range of offensive options to defend critical installations around the country from cyber attacks

Nick Hopkins, defence correspondent
guardian.co.uk, Monday 30 May 2011 21.44 BST



The Government Communications Headquarters (GCHQ), above, is taking a lead role in developing cyber-weapons programme. Photograph: Reuters

The UK is developing a cyber-weapons programme that will give ministers an attacking capability to help counter growing threats to national security from cyberspace, the Guardian has learned.

Whitehall officials have revealed that the UK needs to have a new range of offensive options, and not just bolster defences around the country's critical services and government departments, which regularly come under attack from hackers.

The armed forces minister, Nick Harvey, told the Guardian that "action in cyberspace

UK Developing Cyber-Weapons Programme to Counter Cyber War Threat

will form part of the future battlefield", and though he said cyber-weapons would not replace traditional weapons, he admitted he now regards them as "an integral part of the country's armoury". It is the first official acknowledgment that such a programme exists.

Recognising that there is bound to be concern about when such weapons are used and who would sanction it, Harvey said they would be governed by the same rules that apply to the deployment of other [military](#) assets such as special forces.

"We need a toolbox of capabilities and that's what we are currently developing," he said. "The circumstances and manner in which we would use them are broadly analogous to what we would do in any other domain."

He added: "Cyber is a new domain but the rules and norms, the logic and the standards that operate in any other domain ... translate across into cyberspace.

"I don't think that the existence of a new domain will, in itself, make us any more offensive than we are in any other domain. The legal conventions within which we operate are quite mature and well established."

Though the nature of the weapons being developed remains top secret, it is understood that the Cabinet Office and the Cyber Security Operations Centre at GCHQ have taken the lead on the issue, and that in time there will be some input from the Ministry of Defence. The MoD recently appointed General Jonathan Shaw to head a defence cyber-operations group, and though he does not have an IT background, his experience as a battle-hardened commander from the Parachute Regiment will help refine what might be useful to the military. Shaw told the Guardian cyberspace represented "conflict without borders".

The potential damage caused by highly sophisticated computer [viruses](#) was underlined last year with the discovery of the Stuxnet virus, which successfully disrupted Iran's uranium enrichment programme. The Iranians have accused the Israelis and the US of designing and deploying Stuxnet, which set some of their centrifuges spinning out of control. Experts have described the virus as being so complex and technically advanced that it is "beyond any threat we have seen in the

UK Developing Cyber-Weapons Programme to Counter Cyber War Threat

past". "Someone had the intent to weaponise a virus," said Ilias Chantzou, a security expert.

Though Whitehall officials deny Britain had any involvement in the development of Stuxnet, its discovery added to the urgency of beefing up the country's cyber-defences.

Last year's national security strategy made cyber-security a tier one priority, and an extra £650m was found for it in the strategic defence and security review (SDSR). Harvey told the Guardian that digital networks were now "at the heart of our transport, power and communications systems", and this reliance had "brought the capacity for warfare to cyberspace".

"The consequences of a well planned, well executed attack against our digital infrastructure could be catastrophic ... With nuclear or biological weapons, the technical threshold is high. With cyber the finger hovering over the button could be anyone from a state to a student."

Though Harvey did not specify where future threats might come from, he warned that "it would be foolish to assume the west can always dictate the pace and direction of cyber-technology".

He highlighted how China, for one, is developing "modern militaries and modern technologies".

The foreign secretary, William Hague, told a security conference in Munich in February that the Foreign Office had repelled a cyber-attack a month earlier from "a hostile state intelligence agency". Sources told the Guardian at the time that the attack was believed to be from [Chinese intelligence agencies](#). In his Munich speech, Hague called for agreement on "acceptable rules" for how countries behave in cyberspace.

On Monday night General Graeme Lamb, a former director of UK special forces, told the Guardian that, if anything, the SDSR had not gone far enough in addressing the country's potential vulnerabilities and should have been more radical.

He said that the national security council should have stopped the MoD from

UK Developing Cyber-Weapons Programme to Counter Cyber War Threat

committing "its resources towards a more traditional defence posture".

"The emerging threats we face are ... breathtakingly complicated and far more sinister, far more deadly and far, far more likely [to be used]. Modern technology increasingly allows the individual to bring to bear industrial violence against our citizens previously the exclusive right of states ... complacency has dulled our vision. This reality has for some time been creeping up on us."

Professor Peter Sommer, an expert in technology and security affairs, said that it would not be difficult for GCHQ and other agencies to recast what they were doing to defend against cyber-attacks into a first-strike capability. "Any nation which carefully researches cyber-attack methods for defensive purposes has all the knowledge required for offensive activity. You can also easily argue that a well-targeted attack is low-cost, readily deniable and saves lives by disrupting the enemy. The interesting question then becomes, what are the rules for deployment?"

"I suspect the UK will be borrowing from the doctrines which govern our special forces such as the SAS. It will all be covert but will stop at damaging civilians and assassinating heads of state. And the detailed rules will not be published."

He also warned that the UK was in danger of having "too many overlapping and competing agencies and initiatives".

List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare

List of cyber-weapons developed by Pentagon to streamline computer warfare

By Ellen Nakashima, Published: May 31

The Pentagon has developed a list of cyber-weapons and -tools, including viruses that can sabotage an adversary's critical networks, to streamline how the United States engages in computer warfare.

The classified list of capabilities has been in use for several months and has been approved by other agencies, including the CIA, said military officials who spoke on the condition of anonymity to describe a sensitive program. The list forms part of the Pentagon's set of approved weapons or "fires" that can be employed against an enemy.

"So whether it's a tank, an M-16 or a computer virus, it's going to follow the same rules so that we can understand how to employ it, when you can use it, when you can't, what you can and can't use," a senior military official said.

The integration of cyber-technologies into a formal structure of approved capabilities is perhaps the most significant operational development in military cyber-doctrine in years, the senior military official said.

The framework clarifies, for instance, that the military needs presidential authorization to penetrate a foreign computer network and leave a cyber-virus that can be activated later. The military does not need such approval, however, to penetrate foreign networks for a variety of other activities. These include studying the cyber-capabilities of adversaries or examining how power plants or other networks operate. Military cyber-

List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare

warriors can also, without presidential authorization, leave beacons to mark spots for later targeting by viruses, the official said.

One example of a cyber-weapon is the Stuxnet worm that disrupted operations at an Iranian nuclear facility last year. U.S. officials have not acknowledged creating the computer worm, but many experts say they believe they had a role.

Under the new framework, the use of a weapon such as Stuxnet could occur only if the president granted approval, even if it were used during a state of hostilities, military officials said. The use of any cyber-weapon would have to be proportional to the threat, not inflict undue collateral damage and avoid civilian casualties.

The new framework comes as the Pentagon prepares to release a cyber-strategy that focuses largely on defense, the official said. It does not make a declaratory statement about what constitutes an act of war or use of force in cyberspace. Instead, it seeks to clarify, among other things, that the United States need not respond to a cyber-attack in kind but may use traditional force instead as long as it is proportional.

Nonetheless, another U.S. official acknowledged that “the United States is actively developing and implementing” cyber-capabilities “to deter or deny a potential adversary the ability to use its computer systems” to attack the United States.

In general, under the framework, the use of any cyber-weapon outside an area of hostility or when the United States is not at war is called “direct action” and requires presidential approval, the senior military official said. But in a war zone, where quick capabilities are needed, sometimes presidential approval can be granted in advance so that the commander has permission to select from a set of tools on demand, the officials

List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare

said

Could a Cyber War Turn Into a Real One for the US?

Analysis: Could a cyber war turn into a real one for the U.S.?

By **Phil Stewart**

WASHINGTON | Wed Jun 1, 2011 7:51am EDT

(Reuters) - The United States is warning that a cyber attack -- presumably if it is devastating enough -- could result in real-world military retaliation.

Easier said than done.

In the wake of a significant new hacking attempt against Lockheed Martin Corp, experts say it could be extremely difficult to know fast enough with any certainty where an attack came from. Sophisticated hackers can mask their tracks and make it look like a cyber strike came from somewhere else.

There are also hard questions about the legality of such reprisals and the fact that other responses, like financial sanctions or cyber countermeasures, may be more appropriate than military action, analysts say.

"There are a lot of challenges to retaliating to a cyber attack," said Kristin Lord, author of a new report on U.S. cyber strategy at the Center for a New American Security, a Washington-based think tank.

"It is extremely difficult to establish attribution, to link a specific attack to a specific actor, like a foreign government."

The White House stated plainly in a report last month that Washington would respond to hostile acts in cyberspace "as we would to any other threat to our country" -- a position articulated in the past by U.S. officials.

The Pentagon, which is finalizing its own report, due out in June, on the Obama

Could a Cyber War Turn Into a Real One for the US?

administration's emerging strategy to deal with the cyber threat, acknowledged that possibility on Tuesday.

"A response to a cyber incident or attack on the U.S. would not necessarily be a cyber response ... all appropriate options would be on the table," Colonel Dave Lapan, a Pentagon spokesman, said.

The sophistication of hackers and frequency of the attacks came back into focus after a May 21 attack on Lockheed Martin, the Pentagon's top arms supplier.

Lockheed said the "tenacious" cyber attack on its network was part of a pattern of attacks on it from around the world. The U.S. Defense Department estimates that over 100 foreign intelligence organizations have attempted to break into U.S. networks.

Every year, hackers steal enough data from U.S. government agencies, businesses and universities to fill the U.S. Library of Congress many times over, officials say.

BEHIND THE CURVE

Several current and former national security officials said U.S. intelligence agencies did not appear particularly concerned about the Lockheed attack. One official said that similar cyber attacks directed at defense contractors and government agencies occurred all the time.

Some critics say the Obama administration is not moving fast enough to keep up with the cyber threat or to develop a strategy that fully addresses concerns about privacy and oversight in the cyber domain.

"The United States, in general, is well behind the curve," said Sami Saydjari, president of the privately held Cyber Defense Agency, pointing to "significant strategic advances" out of countries like [China](#) and Russia.

Could a Cyber War Turn Into a Real One for the US?

China has generally emerged as a prime suspect when it comes to keyboard-launched espionage against U.S. interests, but proving Beijing is behind any future plot would be difficult because of hackers' ability to misdirect, analysts say. China has denied any connection to cyber attacks.

The Pentagon's upcoming report is not expected to address different doomsday scenarios, or offer what Washington's response would be if, say, hackers wiped out Wall Street financial data, plunged the U.S. Northeast into darkness or hacked U.S. warships' computers.

"We're not going to necessarily lay out -- 'if this happens, we will do this.' Because again the point is if we are attacked, we reserve the right to do any number of things in response," Lapan said.

(Additional reporting by [Mark Hosenball](#) and [Jim Wolf](#); Editing by Warren Strobel and [Peter Cooney](#))

The Pentagon Is Confused on How to Fight a Cyber War

The Pentagon Is Confused About How to Fight a Cyber War

BY JOHN HUDSON

JUN 01, 2011

Yesterday, the *Wall Street Journal* broke news that the Pentagon decided that cyber attacks against the United States constitute an act of war and may be returned with the full force of the U.S. military. Today, we find out that responding to such attacks is really tricky, and the Pentagon's confused about how to play this 21st-century war game. Here are the stumbling blocks to having a coherent cyber security defense plan:

There are too many attacks to respond to "Every year, hackers steal enough data from U.S. government agencies, businesses and universities to fill the U.S. Library of Congress many times over," U.S. officials tell Reuters. The Department of Defense estimates that more than 100 foreign intelligence organizations have attempted to hack into U.S. networks. Surely the U.S. military is not going to respond militarily to each cyber attack. So the Pentagon's threat runs the risk of appearing empty.

It's difficult to know where the attack came from The Pentagon's 30-page document outlined in the *the Journal* yesterday will be made public soon, largely to serve as a deterrent to others entertaining the idea of striking the U.S. with a cyber attack. But that deterrent strategy might not work given the difficulty of knowing where the attacks originated, notes *The New York Times*. "During the cold war, deterrence worked because there was little doubt the Pentagon could quickly determine where an attack was coming from--and could counterattack a specific missile site or city," writes the paper. "In the case of a cyberattack, the origin of the attack is almost always unclear, as it was in 2010 when a sophisticated attack was made on Google and its computer servers. Eventually Google concluded that the attack came from China. But American officials never publicly identified the country where it originated, much less whether it was state sanctioned

The Pentagon Is Confused on How to Fight a Cyber War

or the action of a group of hackers." A former Pentagon official tells the *Times* "One of the questions we have to ask is, How do we know we're at war? How do we know when it's a hacker and when it's the People's Liberation Army?"

What if other countries adopt our strategy? If regimes opposed to the U.S. also declare cyber attacks an act of war, it could put the U.S. in an uncomfortable situation, notes *Foreign Policy's* [David Hoffman](#). "For argument's sake, let's take the new U.S. strategy that reserves the right to carry out military attacks on anyone who fools with our power grid or nuclear power plants. Let's assume that Iran adopts exactly the same strategy. What would we think if Iran decided to attack the United States--with a missile down a smokestack--in retaliation for Stuxnet?"

It's not clear if the CIA or the Department of Defense is in control Cyber-operations are marked by persistent disagreement over who should take action and under what conditions," [reports](#) *The Washington Post*. The paper details an interesting example surrounding the discovery of Al Qaeda's English-language magazine, *Inspire*, by the Department of Defense. "The head of the newly formed U.S. Cyber Command, Gen. Keith Alexander, argued that blocking the magazine was a legitimate counterterrorism target and would help protect U.S. troops overseas," reports the *Post*. "But the CIA pushed back, arguing that it would expose sources and methods and disrupt an important source of intelligence. The proposal also rekindled a long-standing interagency struggle over whether disrupting a terrorist Web site overseas was a traditional military activity or a covert activity--and hence the prerogative of the CIA."

The attacks can come from state and non-state actors Hoffman adds that "In the nuclear arms race, we knew a lot about our adversaries, if not everything. We set up early warning systems that could track a missile trajectory. We knew where the enemy silos were located. We established 'counterforce' targets that could hit those silos with great precision... The offensive cyber battlefield promises to be far more chaotic than in the nuclear arms race, with many smaller players and non-state actors." The *New York Times* quotes a source close to the administration who says "Almost

The Pentagon Is Confused on How to Fight a Cyber War

everything we learned about deterrence during the nuclear standoffs with the Soviets in the '60s, '70s and '80s doesn't apply."

US Aims Missiles at Hackers

Thursday, June 2, 2011

U.S. Aims Missiles at Hackers

The Pentagon will treat cyberattacks as acts of war—but how will it identify the enemy?

By David Talbot

The Pentagon will soon release a strategy that formalizes a long-articulated position: the United States reserves the right to launch conventional attacks in response to the cyber kind. But figuring out who is behind such attacks may be difficult, or impossible.

"To say that cyberattacks can be acts of war, and that they can be met by kinetic responses, simply confirms a longstanding Department of Defense consensus," says Stewart Baker, a lawyer who was policy chief at the Department of Homeland Security for part of the Bush administration. "Neither of those statements make a strategy, however."

Baker adds that the threat "is much less effective than we'd like, because we largely lack the ability to identify who is attacking us in cyberspace. Until we solve that problem, we might as well claim that we'll respond to cyberattacks by blowing horns until our attackers' fortifications all fall down and their ships all sink."

This problem is illustrated by the famous recent cyberattack involving Stuxnet—a computer worm that damaged Iran's nuclear centrifuges last year.

The Stuxnet worm was a highly sophisticated piece of code that specifically attacked Siemens control systems, causing centrifuges to self-destruct. It leveraged four separate and previously unknown holes in Windows software. And it took care not to damage computers themselves, or other systems.

This technical sophistication, extreme specificity, and lack of other discernible payoff are suggestive of a state-sponsored effort. Many published reports suggest involvement by U.S. and Israeli agents. But as Eric Sterner, a fellow at the George C. Marshall Institute, **argued last year**, a defender could say a competitor to Siemens might have launched the worm, or that intelligence agencies could have let it loose simply to study its propagation.

If something similar were to infect and disable a U.S. nuclear facility or military network, and the United States wanted to strike back, it would be difficult to know whom to strike. However, "we should recognize that perfect attribution is not required,"

US Aims Missiles at Hackers

says Charles Barry, a Vietnam-era combat veteran and professor at National Defense University in Washington, D.C. "We didn't check to see that the Japanese fleet was acting on orders from Tokyo before declaring war on Japan in December of 1941."

In addition to the unsolved attribution problem, Barry says that military planners face challenges in determining what sort of cyberattack "constitutes an act of war." The Pentagon's new cyberwar strategy is expected to declare, in part, that computer attacks on military networks, or attacks that pose hazards to civilians, such as damage to air-traffic control systems or power grids, could be treated as akin to conventional aggression.

Some of these issues will be taken up next week, when military planners and others gather for the annual NATO cyberwar conference in Tallinn, Estonia. That nation was itself the victim of a famous cyberattack in 2007 that highlighted some of the new challenges. The attack commenced after the Estonian government, ignoring protests by Russia, moved a bronze statue of a Soviet soldier that had been installed to commemorate World War II dead.

Soon after, attackers based mainly in Russia launched denial-of-service campaigns against government, media, and telecom Web targets in Estonia, paralyzing them for weeks. The Russian government denied orchestrating the event, attributing it to "patriotic hackers."

If such an event happens again, and it results in loss of life or damage to military systems, the victim nation will need to decide whether to believe such national claims of innocence—or, if it doesn't believe those claims, whether to punish a state for the sins of its citizens.

Meanwhile, there is no agreement within or outside of NATO on how a cyberconflict should play out—including to what extent allies should step in. A **NATO report** chaired by Madeleine Albright last fall noted that large-scale attacks on NATO infrastructure could lead to defensive measures by all members.

The United States created a unified Cyber Command in 2010 to both defend national networks and plan its own cyberattacks if needed. Almost exactly one year ago, General Keith Alexander, who heads the Cyber Command and also directs the National Security Agency, called for **global rules of engagement for cyberwar**. The forthcoming Pentagon report will be a step toward defining those rules, but it may do little to clarify who's playing the game.

US Aims Missiles at Hackers

Chinese Military Scholars Accuse US of Launching 'Internet War'

Chinese Military Scholars Accuse U.S. Of Launching 'Internet War'

by EYDER PERALTA



Peter Parks/AFP/Getty Images

"Faced with this warmup for an Internet war, every nation and military can't be passive," two Chinese military scholars from the Academy of Military Sciences said.

Writing in the Communist Party-controlled China Youth Daily newspaper, two military scholars accused the United States of launching a global "Internet war." [The AP reports:](#)

"Of late, an Internet tornado has swept across the world ... massively impacting and shocking the globe. Behind all this lies the shadow of America," said the article, signed by Ye Zheng and Zhao Baoxian, identified as scholars with the Academy of Military Sciences.

"Faced with this warmup for an Internet war, every nation and military can't be passive but is making preparations to fight the Internet war," it said.

While nuclear war was a strategy of the industrial era, Internet war is a product of the information age, the article said. Such conflicts stand to be hugely destructive, threatening national security and the very existence of the state, it said.

The comments come just days after [Google accused Chinese hackers](#) based in Jinan, China of using a phishing scam to try to acquire the email passwords of hundreds of Gmail users, including senior U.S. government officials. A military vocational school in Jinan was linked to another attack on Google's systems more than a year ago.

[As we reported](#), yesterday, Secretary of State Hillary Clinton called Google's allegations

Chinese Military Scholars Accuse US of Launching 'Internet War'

"very serious." She added the FBI was investigating.

The AP reports that the military scholars did not mention Google in their piece. But the comments also come a few days after [The Wall Street Journal ran a piece](#) in which it said the Pentagon had concluded that a cyber attack could be considered an "act of war."

The Journal reported:

The Pentagon's first formal cyber strategy, unclassified portions of which are expected to become public next month, represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military.

In part, the Pentagon intends its plan as a warning to potential adversaries of the consequences of attacking the U.S. in this way. "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," said a military official.

Latest Hacks Could Set the Stage for Cyberwar

Latest Hacks Could Set The Stage For Cyberwar

by TOM GJELTEN

Listen to the Story

June 6, 2011

In March, unidentified hackers penetrated RSA, a top U.S. cybersecurity company, and stole complex security codes. At the same time, intruders broke into Google's Gmail system and stole passwords, enabling them to potentially gain access to sensitive facilities or information.

In some cases, hackers may be seeking to gain access to a company's computer network simply to have it as a base of operations during a future conflict.

Cybersecurity experts say these recent intrusions are the most sophisticated hacking efforts ever perpetrated against private computer networks. Even more worrisome, such actions could have set the stage for cyberwar. The perpetrators may have gained the capability to identify targets, assess vulnerabilities and position themselves for future attacks.

"I think what we're seeing today are the reconnaissance activities of cyberwar," said Herbert Thompson, who teaches cybersecurity at Columbia University.

Security experts cite several features of the recent attacks as distinguishing them from intrusions more typically attributed to individual hackers. The RSA and Google attacks are both thought to have been carried out by a foreign government, or by actors associated with a foreign government. Both seem to be examples of multistage operations, in which the initial intrusion makes possible subsequent attacks against entirely separate targets.

The theft of RSA security codes, for example, apparently enabled the perpetrators to launch a later attack against Lockheed Martin. The penetration of Google's Gmail accounts may have permitted the intruders to gather intelligence about individuals

Latest Hacks Could Set the Stage for Cyberwar

who could be significant targets during a more ambitious cyberattack in the future.

"We're likely to see a series of these small, subtle battles where the adversary, or the nation state, is gathering information," said Thompson, who is also chairman of his own company, People Security. "It is being done by many large countries, and it's probably an important thing to do. But the big question is: Where is this all headed?"

In some cases, hackers may be seeking to gain access to a company's computer network simply to have it as a base of operations during a future conflict.

"If you have a technology company and a bunch of servers and a lot of bandwidth going to those servers, there's no direct indication that that's a cyberwarfare asset," noted Max Kelly, who investigated cyber-activity as a FBI agent and subsequently served as chief security officer for Facebook. "[But] if a state actor ... gets access to those computers and that bandwidth, they can suddenly use that to attack anywhere in the world, and it's going to look like it came from you."

Kelly, speaking last week at a cybersecurity conference sponsored by the Center for a New American Security, said attackers who gain access to someone's computer system would most likely be content "to just sit there" and wait for an opportunity to use the system to move against someone else.

Cybercrime Versus Cyberwar

With any new theater come new techniques to gather intelligence. New warfighting capabilities are drawn up. That's the phase we're in right now.

- Herbert Thompson, professor of cybersecurity at Columbia University and chief security strategist of People Security

Pentagon officials have generally been careful to separate cybercrime, cyber-espionage and cyberwar. "Right now, what we typically are seeing is criminal activity,"

Latest Hacks Could Set the Stage for Cyberwar

said Robert Butler, deputy assistant secretary of defense for cyber policy. But Butler said his department and other U.S. agencies, in assessing cyberattacks, often struggle to understand "what has happened" and "what type of threat" they are facing.

Some recent attacks are hard to categorize, inasmuch as the goal may be either to steal industrial secrets or to gather intelligence that could be used in wartime.

"When I look at what real cyberwarfare scenarios are going to be, I think they're going to be very much like cybercriminal scenarios," said Kelly. "They [will be] largely covert. If there are actual actions, they will be very targeted actions, for a specific purpose."

In fact, that description could apply to recent intrusions.

"If you just look at cyber as a new theater of war, these are the types of activities that happen in a new theater," said Thompson. "With any new theater come new techniques to gather intelligence. New warfighting capabilities are drawn up. That's the phase we're in right now."

Information Dominance, Naval Intelligence Welcome New Leadership

Information Dominance, Naval Intelligence Welcome New Leadership

(NAVY NEWS SERVICE 1 JUN 11) ... By Joe Gradisher, Deputy Chief of Naval Operations for Information Dominance Public Affairs

WASHINGTON -- Vice Adm. Kendall L. Card assumed the duties of the deputy chief of naval operations (DCNO) for Information Dominance (N2/N6) and director of Naval Intelligence (DNI) during a change-of-charge ceremony at the Pentagon, June 1.

Card succeeds Vice Adm. David J. Dorsett, who will retire following a distinguished 33-year naval career.

Dorsett, the 63rd director of Naval Intelligence, assumed office as the first DCNO for Information Dominance in November 2009. Information Dominance is designated as the lead office for bringing the Navy's intelligence, cyber warfare, command and control, electronic warfare, battle management and knowledge of the maritime environment areas together to align oversight, governance and synchronization mechanisms to deliver end-to-end insight and accountability for Navy information requirements, investments, capability development, and force development.

Under Dorsett's leadership, Information Dominance has now been elevated to a "main battery" in the Navy's arsenal. He has also brought together more than 45,000 military and civilian professionals together to form the Information Dominance Community, tasked with building and operating this main battery.

"It has been the highlight of my career to bring the N2/N6 team and Information Dominance Community together to allow the Navy to capitalize on the opportunities and face the challenges of the information age," said Dorsett. "I've been humbled by the dedication and creativity of the members of our team; they are leaders in a revolution in naval affairs that will assure the Navy is prepared to deal with the changing and growing threats ahead."

Dorsett was born in Roanoke Rapids, N.C., and raised in Virginia. He graduated from Jacksonville University, Fla., in 1978. Following his qualification as a surface warfare officer, Dorsett was designated as a naval intelligence officer. He participated in numerous operations, including Southern Watch, Restore Hope, Desert Fox, Southern Watch Resolute Response, and other sensitive, nationally tasked combat and special operations. As a flag officer he served as special assistant to the Director of Naval Intelligence, director of intelligence, U.S. Pacific Command and director for intelligence, U.S. Joint Staff.

Dorsett graduated with distinction from the U.S. Naval War College and Armed Forces Staff College, and was awarded a master's degree from the Defense Intelligence College.

Prior to assuming the mantle of DCNO/DNI, Card was the director of Concepts, Strategies and Integration for Information Dominance on the N2/N6 staff. He is a career naval aviator with more than 3,900 flight hours in the SH3H Sea King, SH-60F Seahawk, and the S-3A Viking aircraft. He has commanded Helicopter Antisubmarine Squadron 15, USS Rainier (AOE 7) and USS Abraham Lincoln (CVN 72).

As a flag officer, Card has served as director, Command Control Systems, North American

Information Dominance, Naval Intelligence Welcome New Leadership

Aerospace defense Command and U.S. Northern Command; commander, task forces 51/58/59/151/158, Manama, Bahrain; and commander, Expeditionary Strike Group 3.

Card is a native of Fort Stockton, Texas. He earned a Bachelor of Science in mechanical engineering from Vanderbilt University and holds a master's degree in national security and strategic studies from the U.S. Naval War College.

"It is an honor and a privilege for me to assume these duties," said Card. "I look forward to leading the N2/N6 and Information Dominance Community teams as we face all future challenges."

Marine Corps Aviators Depend Upon iPad

Marine Corps aviators depend on iPad

by [Dana Franklin \(RSS feed\)](#) on May 31st 2011 at 2:30PM

Aviators for the United States Marine Corps (USMC) in Afghanistan have ejected heavy stacks of paper charts and grid reference graphics from their cockpits and [replaced them with the iPad](#) according to a report by Tony Osborne for The Shephard Group. The popularity of the [iPad](#) among marine flight crews took off last November when one Cobra pilot figured out how to load digital maps onto the device.

In Afghanistan, identifying compounds and landmarks from the air can be difficult. To eliminate guesswork and better coordinate missions with international ground forces, USMC pilots arm themselves with a plethora of maps of the region. Prior to digitization, paper charts and grids would fill cramped cockpits and require additional training and attention to read correctly. The iPad saves space and allows pilots to search for locations with a few quick taps of their fingers, making it significantly easier for aviators to identify compounds and quickly offer air support.

"It's a game changer," Capt. John Belsha told The Shephard Group. "It's all about sharing situational awareness and using the iPad is much better than using a paper chart."

Work is reportedly underway to integrate the iPad into aircraft in the US to allow Marine aviators to receive flight training with digital maps.

USMC pilots aren't the only group embracing iPads in the cockpit. Earlier this month, Alaska Airlines announced plans to replace various flight, systems, and performance manuals (and eventually paper aeronautical charts) with [digital copies on the iPad](#). Apple's tablet would eliminate up to 50 pounds of paper that its pilots must lug onto every flight.

Is Stealth Dead?

Is stealth dead?

By [Philip Ewing](#) Friday, June 3rd, 2011 8:31 am

A.J.P. Taylor observed that few of the commanders in World War I understood its real strategic dynamics as it was going on. Taught almost exclusively to understand attack — attack, attack, attack — the armies on both sides ground to a bloody deadlock when their rivals always proved stronger in defense. This mystified all sides, but the explanation was simple, he wrote: The railroads meant defending armies could be reinforced and resupplied much faster than they were depleted by forces attacking on foot, through the mud — simply put, defense was mechanized, Taylor wrote, but attack was not.

Fast forward to the 21st century. According to one school of thought, as the U.S. has spent billions of dollars on a relative handful of stealth attack aircraft, potential adversaries can spend millions on sensors and other technology to defeat them by detecting them. Like Taylor's defenders on the Western Front, the defenders have a theoretical advantage: With fixed ground stations, radar aerials can be as big as you want, consume as much energy as you need, and use as much computing power as required. An aircraft has to be able to fly, flight and maneuver, in addition to being stealthy.

Defense analyst Barry Watts takes up this debate [in a new report](#) published by his think tank, the Center for Strategic and Budgetary Assessments, and his thoughtful analysis provides an excellent, detailed primer for stealth skeptics:

In recent years there has been speculation that ongoing advances in radar detection and tracking will, in the near future, obviate the ability of all-aspect, low-observable (LO) aircraft such as the B-2, F-22, and F-35 Joint Strike Fighter (JSF) to survive inside denied airspace. Those taking this view emphasize at least two promising approaches to counter-LO, both of which are being pursued by the Russians, Czechs, and others.

One involves very high frequency (VHF) and ultra high frequency (UHF) radars, which use relatively long wavelengths of about 30 centimeters to six meters. The radar cross section (RCS) of an aircraft not only varies with the wavelength of the radar trying to detect the plane, but the aircraft's RCS is larger for long-wavelength search radars compared to its RCS as seen by the shorter, X-band radars typically used by SAMs for fire-control. Radar physics, therefore, argues that VHF and UHF search radars offer greater potential to detect and track stealthy aircraft.

He continues:

The other promising approach to counter LO has been passive systems such as the Czech VERA-E, which uses radar, television, cellular phone and other available

Is Stealth Dead?

signals of opportunity reflected off stealthy aircraft to find and track them. The main limitation of such systems has been the enormous signal-processing power and memory required to analyze all these emissions, differentiate real targets from ghost signals, noise and clutter, and keep the false alarm rate to manageable levels.

One potential outcome, however, is that as long-wave radars transition to AESAs (and assuming computational power continues to double every two years or so in accordance with Gordon Moore's "law"), information acquisition will overwhelm the capacity of aerospace engineers to reduce platform signatures. The balance between information acquisition and information denial will swing dramatically in favor of the former. **Or, to put the point more bluntly, there will come a time in the not-too-distant future when the SAMs will almost always win against air-breathing penetrating platforms, rendering operations inside denied airspace too costly to bear.**

So does this mean game over for the stealth era? Actually, no, Watts argues. ("there are substantial reasons to doubt this conclusion," he writes.) It's worth reading his report to get his full explanation, but to sum it up, he says advanced new features on the F-35 will enable it to continue enjoying stealth advantages on tomorrow's battlefields: New electronic capabilities, the ability to attack in networked multi-ship groups, and others. This, of course, assumes they all work as advertised.

Watts also assumes tomorrow's defenders get full points for technological rigor, even though they have many technical hurdles to jump before they reach the point where they can see and kill every stealth aircraft.

What do you think?

China, Russia Could Make US Stealth Tech Obsolete

China, Russia Could Make U.S. Stealth Tech Obsolete

- By [David Axe](#)   June 7, 2011 | 7:00 am | Categories: [Air Force](#)
[@daxe](#) · 605 followers



It's been a pillar of the U.S. military's approach to high-tech warfare for decades. And now, it could become obsolete in just a few years.

Stealth technology — which today gives U.S. jets the nearly unparalleled ability to slip past hostile radar — may soon be unable to keep American aircraft cloaked. That's the potentially startling conclusion of a new report from [Barry Watts](#), a former member of the Pentagon's crystal-ball-gazing Office of Net Assessment and current analyst with the Center for Strategic and Budgetary Assessments in Washington.

“The advantages of stealth ... may be eroded by advances in sensors and surface-to-air missile systems, especially for manned strike platforms operating inside defended airspace,” Watts cautions in his 43-page report [The Maturing Revolution in Military Affairs](#) (.pdf), published last week.

That could come as a big shock to the U.S. Air Force, which has bet its future on radar-dodging technology, to the tune of half-a-trillion dollars over the next 30 years. The

China, Russia Could Make US Stealth Tech Obsolete

Navy, on the other hand, might have reason to say, “I told you so.”

That is, if Watts’ prediction comes true — and that’s a big “if,” the analyst admits.

“In recent years there has been speculation that ongoing advances in radar detection and tracking will, in the near future, obviate the ability of all-aspect, low-observable aircraft such as the B-2, [F-22](#) and [F-35 Joint Strike Fighter](#), aka JSF, to survive inside denied airspace,” Watts writes, referring to America’s stealth bombers and fighter jets.

Stealth-killing advances include VHF and UHF radars being developed by Russia and China, and a “passive-detection” system devised by Czech researchers. The latter “uses radar, television, cellular phone and other available signals of opportunity reflected off stealthy aircraft to find and track them,” Watts explains.

These new detection systems could reverse a 30-year trend that has seen the U.S. Air Force gain an increasing advantage over enemy defenses. That phenomenon began with the introduction of the F-117 stealth fighter in the late 1980s, followed by the addition of the stealthy B-2 (pictured) in the '90s and, more recently, the F-22.

So far, the Air Force has only ever fielded a few hundred stealth aircraft, requiring it to [constantly upgrade](#) some nonstealthy fighters. But the flying branch plans to purchase more than 1,700 F-35s (at more than \$100 million a pop) from Lockheed Martin in coming decades, plus up to [100 new stealth bombers](#). In that sense, the stealth era is only now truly dawning — just as effective counter-measures are nearly ready, Watts points out.

In that sense, the Air Force’s stealth gamble could turn into very, very long odds.

China, Russia Could Make US Stealth Tech Obsolete

Comparatively, the Navy has played it safe. At the same time the Air Force was investing its research and development dollars in stealth, the Navy has taken a different approach to defeating enemy defenses. Where the Air Force plans to slip past radars, the Navy means to jam them with electronic noisemakers or destroy them with radar-seeking missiles. That's why the [only radar-killing planes](#) in the Pentagon inventory belong to the Navy — and why, until the forthcoming F-35C, the Navy has never bought a stealth fighter.

Nowhere is that philosophical difference more apparent than in the Pentagon's on-again, off-again effort to develop [jet-powered killer drones](#). The [Navy's X-47 drone](#), built by Northrop, is minimally stealthy. [Boeing's Phantom Ray](#), intended mostly for Air Force programs, is arguably as stealthy as an F-35 in certain scenarios.

There's still a chance the Air Force's bet on stealth could pay off, Watts writes. That largely depends on two capabilities planned for the F-35.

First, there's "the JSF's sensor suite and computational power," which Watts explains "can be easily upgraded over time due to the plane's open avionics architecture, giv [ing] the F-35 an ability to adjust its flight path in real time in response to pop-up threats, something neither the F-117 nor the B-2 have been able to do."

Second, the F-35's radar, a so-called "electronically scanned array," could in theory be used to jam an enemy radar or even [slip malicious software code](#) into its control system.

Neither of these capabilities is actually a form of stealth, per se. Rather, they would *complement* the F-35's ability to absorb or deflect radar waves. Described uncharitably, the Air Force has had to add nonstealthy skills to its stealth fighters, just to help them survive.

China, Russia Could Make US Stealth Tech Obsolete

Watts doesn't address one other way the Air Force could preserve its stealth advantage: by speeding up the development of drone aircraft — which, by virtue of their smaller size, have the potential to be much stealthier than any manned aircraft.

It's also worth noting that America's biggest rivals don't doubt the continuing relevance of stealthy planes. [Russia](#) and [China](#) have both unveiled new stealth-fighter prototypes in the last two years.

The way Watts describes it, the “end of stealth” is just one of the many big changes that *could* occur in near-future warfare — big emphasis on “could.” “The honest answer to the question about how fundamentally war's conduct will change — and how soon — remains: It depends.”

Photo: B-2 stealth bomber (U.S. Air Force)

Killer App: Army Tests Smartphones for Combat

Killer App: Army Tests Smartphones for Combat

By [NATHAN HODGE](#)

The Army plans to hold desert trials in the U.S. next week to test off-the-shelf iPhones, Androids and tablet computers for use in war.



The Army plans to hold desert trials in the U.S. next week to test off-the-shelf iPhones, Androids and tablet computers for use in war. Nathan Hodge has details.

Starting Monday, the Army will also stress-test a variety of applications that could allow troops to tap digital information from the front lines—for instance, streaming video from a surveillance camera, or downloading up-to-the minute information from a remote database.

The Army doesn't have a plan to give every soldier a smartphone. But Gen. Peter Chiarelli, the Army's vice chief of staff, recently said that if the devices proved themselves in testing, the service would "buy what we need for who needs it now."

Many of the applications the Army wants to develop—for instance, the ability to watch full-motion video shot from a drone—can already be done with

Killer App: Army Tests Smartphones for Combat

equipment now in the field. The potential advantage of smartphones and tablets is their lighter weight and ease of use.

The tests will take place at the White Sands Missile Range in New Mexico and at neighboring Fort Bliss, Texas, as part of a wider Army evaluation of a range of communications gear. During the six-week event, soldiers of the Second Brigade Combat Team, First Armored Division, will see if the equipment holds up in rugged desert conditions.

[View Full Image](#)



U.S. Army

Soldiers of the Army Evaluation Task Force testing the military usefulness and functionality of smartphones late last year at White Sands Missile Range, N.M.

Michael McCarthy, one of the Army's project leaders, said the point of smartphone testing is to see what works and what doesn't. "We want to give people the right phones for the right reasons, not just give them another shiny thing to hang on their equipment carriers," he said.

Army officials say the devices need to be relatively affordable, perhaps costing a few hundred dollars each, depending on the model. The service doesn't want to "spend \$2,500 to ruggedize a \$200 phone," Mr. McCarthy said.

In theory, smartphones could eventually become common tools for troops, with software customized for each unit or mission. The Army, for instance, is testing apps that could expedite the treatment of soldiers wounded in

Killer App: Army Tests Smartphones for Combat

combat. In the coming exercise, the service will evaluate several apps that help speed requests for medical evacuation by relaying the exact location of an injured soldier, with touch-screen menus to fill in crucial information such as the patient's name, health status and type of injury.

Another app, called "SoldierEyes," turns a smartphone into a sort of battlefield navigation device. In addition to displaying a digital map, it features an "augmented reality" mode that enables the user to flip on the camera and scan the horizon. Digital markers pop up on the screen, displaying the direction and distance to objectives on the battlefield.

Biometrics—where the photos, fingerprints and iris scans are used to verify a person's identity—are another possible application for a military smartphone. The military already uses portable biometric collection kits to identify suspected insurgents in Iraq and Afghanistan, but a downloadable phone app would, the thinking goes, put that kind of tool in the hands of more soldiers.

The Army is experimenting with Apple Inc. devices such as the iPhone and iPad, but is also trying devices built around Google Inc.'s Android operating system. All told, the Army has identified around 85 digital apps for testing, some created by commercial software designers, and some developed in-house by soldiers. The service is also developing downloadable apps to substitute for bulky instruction manuals that need constant updating, often at considerable cost.

To date, the Army has invested about \$4.2 million in the development of military apps and the study of smartphone technology.

Troops need power to recharge their devices, and so the Army is studying alternative power sources, including solar chargers and micro fuel cells. Equally important, smartphones need enough network bandwidth to relay everything from chat and text messages to streaming video.

Killer App: Army Tests Smartphones for Combat

Brendan O'Connell, who heads a military-business unit for radio manufacturer Harris Corp., says smartphones are a popular subject in defense-technology circles, but that effective cellular networks for the troops aren't feasible without a "backbone communications architecture" that is rugged, mobile and secure.

"We don't want to get anybody hurt or killed by letting information out," said Rickey Smith, of the Army Capabilities Integration Center. Limiting weight is also key. "If it adds an ounce of weight to a soldier, make sure you need it," Mr. Smith said.

The devices themselves will also have to take a beating. On that score, however, Mr. McCarthy said the durability of commercial smartphones had been a "pleasant surprise," with hundreds of phones surviving handling by soldiers.

"In the last year, we've only had one that was damaged, and it was dropped on a carpeted floor and broke into three pieces," he said. "The major who did it has gotten infinite grief from his peers."

Navy Should Wait to Implement UCore

Rand: Navy should wait to implement UCore

June 7, 2011 — 10:37pm ET | By [David Perera](#)

The Navy should hold off from requiring widespread implementation of UCore as a means of achieving interoperability between information systems, says Rand Corp. in a new report.

The report, posted online June 2, lauds UCore for its potential to significantly improve defense data interoperability, but says that potential concerns over its bandwidth consumption and lack of maturity should result in further DoD pilot projects rather than extensive service-wide implementation. The Rand study was co-sponsored by the Navy, but many of its findings appear generalizable to all military services.

UCore is an XML-based schema for situational awareness data developed by the federal government and military; developers released version 2.0 in March 2009. Rand says UCore differs from other metadata schemes in that it's possible to embed pre-existing XML schemas into a UCore data package, meaning that while a system capable of processing only UCore messages wouldn't be able to interpret the legacy XML metadata, end users would at least be aware that it exists.

UCore elements are limited to *who*, *what*, *when* and *where*, the report says, but extensions could be developed. The report particularly applauds the fact that UCore extensions themselves are extensible. That means that UCore could lead to layered data exchanges in which the higher levels consist of commonly accepted, fixed elements but which are extended in greater detail at lower levels, allowing programs to "innovate with extensions and continue to evolve their data exchange formats."

However, at least in the Navy, adoption of UCore's *who* and *what* elements could require significant changes to database structures, the report says. "These data elements are likely to be defined in different ways in Navy systems and to represent a large taxonomy of object names and attributes."

The report also includes a warning about extensibility, since other studies have found that metadata tagging can increase message size by more than an order of magnitude. For high bandwidth networks, that's no problem, but at the tactical edge where communication links depend on satellites or line-of-site communication links, UCore messaging could significantly degrade network performance, the report says.

The size of UCore messages would depend on how it's implemented the report notes--

Navy Should Wait to Implement UCore

whether legacy metadata is transmitted or not, for instance--and the Defense Information Systems Agency has investigated metadata compression schemes, the report says. Nonetheless, because UCore has yet to be tested on a tactical network, the report recommends further study.

The development of official extensions, such as planned C2Core (the C2 is for "command and control") are also needed to make UCore a more useful tool, the report adds.

For more:

- [download](#) the report, (.pdf)

Navy Focuses on IT Efficiency: 'Overarching' Networking Strategy On Hold

Navy Focuses On IT Efficiency; 'Overarching' Networking Strategy On Hold

(INSIDE THE NAVY 30 MAY 11) ... By Andrew Burt

A Navy information technology networking strategy, months past its February 14 deadline assigned by Under Secretary Robert Work, has been placed on hold so that the department can focus more of its energy on high-priority IT efficiency efforts currently in the works.

The strategy, called the Naval Network Strategy (NNE) document, was originally assigned in a Dec. 3 memo Work sent to the Navy' chief information officer.

"The document has been delayed in order to ensure our IT/Cyberspace efficiency efforts are fully aligned with where we want to go [in the] long term, which will be detailed in the NNE strategy," wrote Michael Jacobs, the director of enterprise architecture and emerging technology for the Navy, in a May 24 email. "Rather than rush the strategy, which is a long-term vision document, we have focused on efficiency efforts targeted for execution and implementation during the next 24 months."

The efficiency efforts were outlined in an IT campaign plan released earlier this month.

"Reducing data centers and rationalizing applications, which are efforts listed in the Campaign Plan, will contribute to reducing network complexity and enabling a higher level of configuration control," wrote Jacobs. "This will better enable us to move forward with a true enterprise information environment, which is the overarching goal of the NNE Strategy."

In his memo, Work wrote that "governance, administration, operation, investment and acquisition of [Navy IT] resources and assets will be predicated" on the NNE strategy.

"NNE shall be aligned with DOD efforts, and will become the Department of the Navy's net-centric environment that securely and efficiently leverages the full range of information resources," he wrote. "It will function as a key enabler to providing rapid, on-demand, ubiquitous access to authorized users and systems in support of the Joint Information Environment, all [Navy] business systems, and where applicable will be used to guide Navy and Marine Corps strategic planning for operational IT/cyberspace systems."

'Ruthless' Cost Cutting Coming to Navy IT

'Ruthless' Cost Cutting Coming To Navy IT

(FEDERAL NEWS RADIO 09 JUN 11) ... Jared Serbu

The Department of the Navy's chief information officer said Navy and Marine Corps IT managers should expect to see "ruthless" internal cost cutting this year in preparation for significant budget cuts.

"We don't know how much that is yet, but it's going to be a big number," Terry Halvorsen said at the DON CIO's May 12 conference in Virginia Beach, Va. "There's no way it can't be a big number."

Halvorsen's office [posted an audio recording](#) of the session on its website this week.

To achieve the cost reductions, he said, he's gotten the word from as high as the Secretary of the Navy that if the department is going to take risks with its IT systems, they shouldn't be the ones that directly provide warfighting capability. Instead, he said, the Navy and Marine Corps need to accept risk in their business systems as they look for ways to do things better and cheaper.

"And I fully understand sometimes it's difficult to separate business IT from the rest of IT and from warfighting IT," he said. "But I think we're going to have to make some attempts to do that. We're going to take risk. The one thing I don't want to do is to take risk when we don't have to in any area that affects, call it the tip of the spear, the edge of the battle, the thing that we are in business to do. It is to kill the enemies of the country. That is the business of this corporation if you wanted to put it in business terms."

He said the DON will take a ruthless approach to finding savings in the short term rather than relying on promises of future cost reductions.

"We spend X amount of dollars today. We are going to spend X minus amount of dollars next year," Halvorsen said. "Savings are what we take away. Does that mean we won't look at cost avoidance plans? No, we'll certainly do that. But when we do that, DON's going to be very ruthless in saying, 'OK, we gave you two dollars. You said if we gave you two dollars, in the next year, you would save us four. Not cost avoid, not maybe. You said you'd save us four. We're taking the four.' We are going to be ruthless, because if we don't do it, I guarantee it's going to be done for us."

The first job is getting a handle on how much the Navy and Marines actually spend on IT, something he said his office has been working closely on with the department's financial managers. But Halvorsen's office has identified cost centers that are prime candidates for efficiency gains. They are the usual suspects in government IT: underutilized data centers, expensive, customized software, exploding bandwidth demands, inefficient software licensing practices and huge numbers of duplicative applications on the department's networks.

"We run at least seven—and maybe nine depending how you define them—records management and tasking systems," Halvorsen said. "We are going to one. It makes no sense. I get that they may be meeting somebody's requirement. The question is, is the requirement for maybe a small number of people worth the additional money that we're paying across the board? Not just in the cost of buying that new system, but the cost of sustaining it, operating it and securing it. I'm

'Ruthless' Cost Cutting Coming to Navy IT

going to tell you the answer on that one is no. Records management is important, but if I miss something on records management, do you think anything happens to a Marine in the field? I don't either."

Halvorsen said the Navy and Marine Corps will set specific targets for removing applications from their inventory. As of now, they estimate there are close to 2,000 on the department's three main networks.

"We are going to not just put some controls on applications," he said. "We are going to put a money target that says X percent or X dollars worth of applications come of the system in fiscal year 2012. We're going to call it application rationalization, and it will be maybe one of the more unpopular things that's going to happen, but it's going to happen."

The prime targets will be applications or systems that overlap with one another.

"We run multiple systems that basically do the same thing because someone said they can't change their process," he said. "Well, we're going to do the math. And if the math says this 100,000 people are costing us an additional 25 percent against the 1.2 million people we serve, that system is gone. It's a math drill, and we take the money. You are going to see a lot of that this year."

The department already has started to tackle its software licensing costs through an enterprise software licensing program run by the Marine Corps. They've already set up a contract vehicle for Microsoft products, and others are coming soon. Halvorsen said those vehicles will be the only authorized method to buy a given license.

"There will be no waivers to that," he said. "One of the things we're going to have to do as part of our efficiencies is enforce that, and not allow the waivers we've allowed in the past. People with good intentions have gone around that in the past, but we end up, when you pull the string, paying more than we should have."

The department began heading in the direction of data center consolidation early this year when it imposed a moratorium on the construction of any new data centers. DON currently has between 140 and 170, depending on what counts as a data center. The department has closed five this year, and plans to have fewer than 100 by 2013.

Janice Haith, who serves as the CIO for the Navy portion of the DON, said for now, the consolidation effort only includes centers in two environments: the Navy Marine Corps Intranet (NMCI), and the Space and Naval Warfare Systems Command (SPAWAR).

"That is purposeful," she said. "We have excess capacity and we need to use it. We're going to continue to go down the path of consolidation, and the savings are not just people. There's an energy savings we're trying to calculate, because that's another of the areas that the secretary is concerned about."

Through all the cost saving efforts though, Halvorsen said the bottom line is that the DON needs to save money now, not just in the future. He said that's something he wants members of industry to keep in mind when they approach the department with ideas that could lead to efficiencies.

"When you say you're going to save us money, understand what you saying," he said. "You

'Ruthless' Cost Cutting Coming to Navy IT

said I'm going to spend less money today. If you say 'you could spend less money if you give me more money,' OK, we'll listen to that, but let me be very clear. The people who will get more response are the people who say, 'hey, I have a way today that you could spend less money and still retain your service.' This is about spending less money."

[Listen To Audio](#) (RT: 7:04)

Navy Needs a Way to Handle UAV, Sensor Data

Navy Needs A Way To Handle UAV, Sensor Data

TCPED key to operating networks anytime, anyplace, official says
(DEFENSE SYSTEMS 09 JUN 11) ... Amber Corrin

One of the biggest hurdles for current and future naval operations is the data challenge: the ability to strategically gather, examine and share information amid the data deluge emerging from widespread sensor use.

To deal with the challenge, the Navy must implement proper procedures for tasking, collection, processing, exploitation and dissemination, or TCPED, of the information, a top official said June 9.

“It’s not just about collecting information for intelligence purposes behind black doors. It’s about what information do I want to share ... and with who?” said Dave Weddel, assistant deputy chief of naval operations for information dominance, at the AFCEA Naval IT Day in Vienna, Va.

Weddel said that TCPED is integral to meeting the needs of a growing unmanned aerial vehicle force that is yielding volumes of data – needs that will require greatly improved automation capabilities because the data deluge overwhelms human capabilities. He pointed out that the explosion of UAV and sensor use is resulting in a 1,000 percent increase in afloat bandwidth demand – and that TCPED must be able to be carried out even in the most disconnected of environments, such as when satellites are not available.

“One of the main principles is TCPED is we need to be able to do it regardless of the amount of bandwidth we’ve got,” Weddel said. “We need to have the agility ... to fight through an attack.”

He pointed out some key gaps in TCPED capabilities, including the ability to exploit and disseminate quantities of sensor data, as well as the ability to leverage joint and international coalition partners and effectively managing enterprise networks.

He also said data processing and exploitation need to be better aligned, and that there needs to be more dynamic support for multi-mission requirements.

Manpower is another major issue, Weddel noted.

“The number of people aboard our ships is going down, but the amount we’re asking them to do is growing ... how do we keep up?” The Navy may need to rethink the way it trains the next generation of sailors, he said.

“What kind of Navy do we want to be? What kind of missions does our country want us to do?” Weddel asked, adding that these questions must be considered when it comes to facing a budget crisis and key decisions. “We’ve got to work together. The threats are only increasing.”

Marines Buying \$880 Million Worth of PCs, Laptop and Tablet Computers

Marines buying \$880 million worth of PCs, laptops and tablet computers

BY BOB BREWIN 06/08/2011

The Marine Corps has kicked off a massive purchase of more than 400,000 desktop and laptop computers, valued at \$880 million, under a contract that also requires a smaller number of commercial and rugged tablet computers.

The service wants to buy the bulk of the gear -- 131,965 general purpose laptops and 141,838 desktop computers -- through a five-year Marine Corps Common Hardware Suite [procurement](#) announced Monday.

The Marines will also use the contract as an umbrella vehicle to acquire 7,220 commercial tablet computers and 7,880 rugged tablet computers as well as 15,850 small, lightweight netbook computers.

Retired Army Maj. Gen. Dennis Moran, who now works for Harris Corp., said the planned Marine bulk buy of tablet computers though small will prove to be the wave of the future for tactical computing. Moran, who served as deputy director for command, control and computer systems on the Joint Chiefs of Staff before retirement, said tablets are ideal for viewing maps and other graphic information.

Moran predicted that tablets will be used throughout infantry units, eventually down to the platoon and squad levels. He said the Army will test tablet computers later this month in a large-scale tactical network [exercise](#) at the White Sands Missile Range in New Mexico.

The Marines said they plan to use this massive buy to establish a standardized computing equipment environment for deploying units and also to provide equipment for domestic organizations that will be connected to the Navy's Next-Generation Network. Equipment purchased for units that deploy will require global logistics support, the request for proposals said.

Security is another key requirement of the procurement, and the Marines told bidders that it did not intend to purchase any computers that include Bluetooth short-range wireless -- a standard built into commercial PCs -- and they also must provide the capability to disable other forms of wireless communications, including Wi-Fi, radio frequency identification and GPS.

The Marines have the Common Hardware Suite procurement on a fast track, with bids due July 22.

China's PLA Bans Soldiers from Social Media

China's PLA Bans Soldiers From Social Media

AGENCE FRANCE-PRESSE

Published: 1 Jun 2011 08:36

BEIJING - Making online friends could play into the hands of the "enemy", according to China's People's Liberation Army, which has said its roughly 2.3 million soldiers will be banned from using social media.

The world's largest military force has notified service men and women that it will strictly enforce the ban to "safeguard military secrets and the purity and solidarity" of the PLA, state media said this week.

The People's Liberation Daily, the armed forces' official newspaper, said passing on personal details such as a soldier's address, duties or contact details could risk revealing the location of military bases.

It added that particular risks exist in users posting photos of themselves, such as during training, which could divulge military capabilities and equipment.

The ban was included in regulations announced last year that proscribed soldiers from launching websites or writing blogs, the paper added.

But in a sign that the ban was apparently being ignored in a country where social media are wildly popular, the military brass has taken the step of re-emphasizing the restriction, warning of a "grim struggle" on the Internet.

Officers and soldiers must be made to understand the "real dangers" of making friends online and to "strengthen their knowledge of the enemy situation," it said, without elaborating.

China has nearly half a billion online users, according to official figures, and Chinese-language social media sites similar to Facebook and Twitter - which are blocked by the country's censors - count hundreds of millions of users.

China's PLA Bans Soldiers from Social Media

The newspaper last week said China's military has set up an elite Internet security task force tasked with fending off cyberattacks, while denying that the initiative is intended to create a "hacker army."

The United States, Australia, Germany and other Western nations have long alleged that hackers inside China are carrying out a wide range of cyberattacks on government and corporate computer systems worldwide.

US Navy Calls On Video Gamers for Strategic Help

U.S. Navy Calls on Video Gamers for Strategic Help

Posted: 6.1.11



US Navy Calls On Video Gamers for Strategic Help

The U.S. Navy is turning to the video-gaming public to track and fight pirates. Massively Multiplayer Online War Game Leveraging the Internet, or MMOWGLI, is an interactive message board where players collect points by presenting their ideas and getting votes from other players.



The U.S. Navy is reaching out to gamers for suggestions on how to track and fight modern-day pirates.

In the virtual world of online gaming, players can acquire skills that allow them to slay fire-breathing dragons, build elaborate civilizations and terminate mobs of hungry zombies. But what if you could translate these gaming skills into real world tactics and fight actual modern-day pirates?

That is the idea behind the U.S. Navy's online war game. The game outlines scenarios, such as pirate ships holding valuable hostages off the coast of Africa, U.S.-Chinese relations at a breaking point where both countries have naval ships in the area.

Players come up with a 140-character suggestion for tools to fix the situation. Then, players are asked to identify (also in 140 characters) what risks could be detrimental to the proposed solutions.

Anyone can participate in the game, submit their own suggestions and vote on ideas from other players. The first round of cuts will take place after the first week of play and the lowest-voting ideas will be eliminated. At the end of the

Army Seeks Social Media Gurus to Save Afghan War

Army Seeks Social Media Gurus to Save Afghan War

- By [Spencer Ackerman](#)   June 8, 2011 | 4:53 pm | Categories: [Info War](#)
[@attackerman](#) · 10.7K followers

Know how to Tweet? Or how to put words into the mouths of foreign security functionaries? If so, the U.S. Army wants you to help un-quagmire the Afghanistan war. A new solicitation from the Army seeks communications experts to run the full spectrum of outreach and messaging for the war effort. A new “Web Content/Social Media Manager” will work with the U.S. military command in Afghanistan, known by the acronym USFOR-A, to spruce up and maintain “[the command’s official website and related social media platforms, such as Facebook, Twitter, YouTube and Flickr.](#)” (PDF) Other officials will dig into the Afghan security ministries to advise key officials how to convince people they’re competent, energetic and not at all corrupt.

To non-Afghan eyes, USFOR-A’s got a pretty robust social media presence. Check out how often [it tweets its messaging](#) into the ether. Its [YouTube channel](#) is filled with positive videos, and its Facebook page — [folded into the NATO command’s page](#) — has nearly 80,000 Likes. Is the war won yet?

Evidently not. The solicitation sees the Taliban doing a better communications job than the U.S.: “To date, the Insurgents (INS) have undermined the credibility of USFOR-A, the International Community (IC), and Government of the Islamic Republic of Afghanistan (GIRoA) through effective use of the information environment, albeit without a commensurate increase in their own credibility.” Guess the Army thinks the Taliban’s [recent English-language tweeting](#) and [SMS terror campaign is having an impact](#). Or that Gen. Stanley McChrystal’s 2009 plea to [revamp the war’s communications apparatus](#) didn’t have the desired effect.

Army Seeks Social Media Gurus to Save Afghan War

That problem's magnified when it comes to the Afghan government, which is so corrupt that Ryan Crocker, Obama administration's nominee for ambassador to Kabul, compared its perfidies to a "[second insurgency](#)" on Wednesday. The answer? "[C]ulturally-astute and culturally-attuned communication and public affairs advisement" to mouthpieces for the ministries of Defense and Interior.

What will those advisers do? The short answer is teach them how to spin. The long answer: "better align media reporting and public perception and proactively engage opinion-shapers, from media to key leaders, in order to bring these attributes of the information landscape into alignment."

This is only partially about gaining or keeping Afghan support. The bolstered social media push needs to have rapid translation into Dari and Pashto, as well as ceaselessly nimble translations of the local press so the military gets feedback, the solicitation says. But it's primarily to "inform key audiences" — that is, "media and civilian populations internationally and within the region" about USFOR-A spin. And when the best that the smooth diplomat Crocker can tell the Senate about the war is that it's "not... hopeless," it's no wonder that the Army thinks USFOR-A needs all the communications help it can get.

Data Grows, and So Do Storage Sites

Data Grows, and So Do Storage Sites

By VERNE G. KOPYTOFF

Published: June 5, 2011

SAN FRANCISCO — When people had only one or two computers, file sharing wasn't a big worry.

Now, gaining access to personal files is a chore for people who own an arsenal of computers, smartphones and tablets.

The annoyance of e-mailing documents to themselves or saving their work to a thumb drive has given new life to an old idea — online storage. People simply save their Word documents, spreadsheets and photos in “the cloud,” a Web-based file cabinet accessible from any device that has an Internet connection.

A number of companies focused on online storage are quickly gaining users and attention. New investment is driving a boomlet in the niche business, adding to an already lengthy list of competitors: Dropbox, YouSendIt.com, Cx.com, Box.net, 4Shared and SpiderOak. Apple may do something similar with its iCloud service, to be introduced on Monday.

Google began acclimating people to the notion of storing documents in the cloud with its Google Docs feature in 2005.

And online backup or storage services like MobileMe from Apple, Windows Live SkyDrive from Microsoft, Mozy from EMC and SugarSync are now familiar. What's changed is that more people have discovered a need for them.

Aaron Levie, chief executive of Box.net, an early online storage company based in Palo Alto, Calif., said that the increased adoption of mobile devices and ubiquity of online

Data Grows, and So Do Storage Sites

connections had created a bigger need for companies like his.

Nearly 60 percent of adults with online access own at least two Internet connected devices, according to Forrester Research. Just under 3 percent, or 4.5 million people, have at least nine different gadgets. If that seems to be a lot, think about this: a person may have a home computer and a work computer, and other members of the family may each have computers. Then count smartphones and tablets, and it's not hard to get to a large number of machines.

"It just sort of clicked," Mr. Levie. "There ended up being a tremendous amount of interest."

"Our vision is to simplify millions of peoples' lives," said Drew Houston, chief executive of Dropbox, where 25 million users upload files at the rate of 300 million a day. "You don't have to worry that you have some files on your Mac, some stuff on your work computer and then some more on your [iPhone](#)."

A growing number of people believe him. Dropbox stores 100 billion files on its servers. Box.net says it has six million users while Mozy says it has three million.

Meanwhile, storage companies benefit financially from a constant decline in costs as servers and data storage devices get cheaper each year. Leasing server space is five to eight times cheaper than when Box.net started in 2005, Mr. Levie said.

The sales pitch for online storage is that it lets users make changes to a Word file, for example, so that there is a single version available from both their work and home computers. It is a process known as synchronization, or sync for short. Users can also collaborate on a documents with colleagues or share video clips and photos with friends.

Many online storage services let users store a minimal amount of data free of charge. For

Data Grows, and So Do Storage Sites

more space, users pay up to \$20 a month. (Dropbox gives users who enlist more customers additional storage.) Saved files are accessible from any Internet connected device.

Backing up files is a side benefit. Users no longer risk losing their children's photos if they forget their mobile phone in a cab or their homework if their hard drive crashes.

George Hamilton, an analyst with Yankee Group, said that online storage largely appealed to tech-oriented consumers, although it has been gaining more mainstream adoption recently.

But one thing still gives most consumers the willies: security. While there are no known cases of purloined or exposed documents on these services, well-publicized hackings and thefts at big companies like Sony, RSA Security and the e-mail marketing firm Epsilon Data Management worry the late adopters. "I wouldn't want to put anything with a [Social Security](#) number on a cloud-based storage service," said Mr. Hamilton.

A security expert did recently complain to the Federal Trade Commission about how Dropbox encrypted files on its service. Dropbox's employees could get access to unencrypted files, he said, and he accused the company of failing to disclose this.

Mr. Houston called the criticism a "rite of passage" and emphasized that Dropbox takes security very seriously, including prohibiting employees from rooting through user files. However, the company, like any other, must turn over data if it is legally required to do so.

In general, Dropbox likens its protections to what banks and the military use. Files saved with Dropbox are encrypted during transmission to Amazon.com's servers, which the company leases. After reaching their destination, those files are divided into discrete

Data Grows, and So Do Storage Sites

blocks, no bigger than a few megabytes. Those blocks are then individually encrypted in storage.

Mr. Houston says he saves nearly everything to Dropbox including copies of his driver's license and passport.

"I have five or six laptops, and they are totally interchangeable," he said.

The field is flooded with competitors in part because no one company has a clear advantage in the market, which spans both consumers and business customers.

Two months ago, Amazon introduced Cloud Drive for storing all kinds of files, including digital music. Cx.com, another service, premiered in January with financing from TomorrowVentures, a [venture capital](#) company controlled by Eric E. Schmidt, Google's chairman and former chief executive.

Brad Robertson, chief executive of Cx.com, which has around 200,000 users and which is free as it tests its service, said he was not intimidated by all the competition. Focusing on security will help set his company apart from rivals, he said.

"If you take search or e-mail, or any feature where you have new products in the marketplace, you have a while before each one finds its uniqueness," said Mr. Robertson, whose company is based in Palo Alto, Calif. He acknowledged that eventually "some get gobbled up and go away."

Intel, Apple & the Transformation of the PC

June 05, 2011

Intel, Apple & the Transformation of the PC



If you're a PC and gadgets fan, then June is turning out to be quite the interesting month. Intel delivered a series of keynotes at Computex 2011 last week and Steve Jobs will be bringing the house down tomorrow when he takes the wraps off their latest operating system upgrades dubbed OS X Lion and iOS 5. Apple's blowout news of course will come from revelations about their all-new iCloud music service. In today's report, we'll take a look at some of the interesting new features that will be coming to our personal computers over the next 18 – 30 months. Intel presented some real surprises, especially their 2013 processor which is a whole new from scratch architecture. I liked what I saw on the way from Intel and I'll be thrilled to see what Apple delivers tomorrow. What a great month it's turning out to be for tech heads!

Clashing Views: The Future of the PC

A major clash of views emerged in the press last week between Intel and Apple concerning the future of the PC. It began with keynotes from Intel's Sean Maloney and Mooly Eden at Computex 2011 in Taipei Taiwan on Tuesday May 31. At that time Intel openly admitted that a major transformation of the PC was being undertaken but that in context, it was simply the third such transition since the mid-ninety's: No more – no less.

Intel, Apple & the Transformation of the PC

In contrast, Apple's Tim Cook, according to Bill Shope of Goldman Sachs, stated that he saw "no reason why the tablet market shouldn't [eclipse the PC market](#) over the next several years." Being that Apple's World Wide [Developer Conference](#) begins tomorrow with the promise of delivering the goods on OS X Lion, iOS 5 and their new music cloud services – it was understandable why Cook was being so optimistic. Yet both companies are simply preaching for their own parishes or posturing for the media's attention.

There's no doubt that Apple currently has the wind at their back and that they're riding a massive wave of momentum due to the iPad. And with what will be coming out of Apple's developer conference tomorrow will only take more oxygen out of the PC world's balloon.

Yet to be fair, Intel did make a decent case for the PCs coming transformation in Taiwan last week – and a lot of what was being described could very well end up in future Macs: So not all was a loss. The problem, however, was that their vision was lackluster.

There's no doubt that Intel's customers are desperate to find that silver bullet that will finally blow out Apple's tires. Yet such a bullet will likely take another two or three years to emerge, according to Intel's own roadmap, and that's why leading PC companies like HP are being forced to leave the Mother Ship at this point in time so as to fill in the gap and take on Apple directly, *now!* HP's WebOS and upcoming tablets promise to deliver a quality alternative to the iPad and have their own music cloud surprises to take on Apple's forthcoming iCloud services later this summer: But that's another story for another day.

For today, our report will provide you with interesting new factoids, insights and a ton of interesting presentation slides to help you visualize the current and future states of the PC so as to help provide you with a balanced look at where personal computing is going, according to the Book of Intel.

Emerging Markets are Growing PC Growth

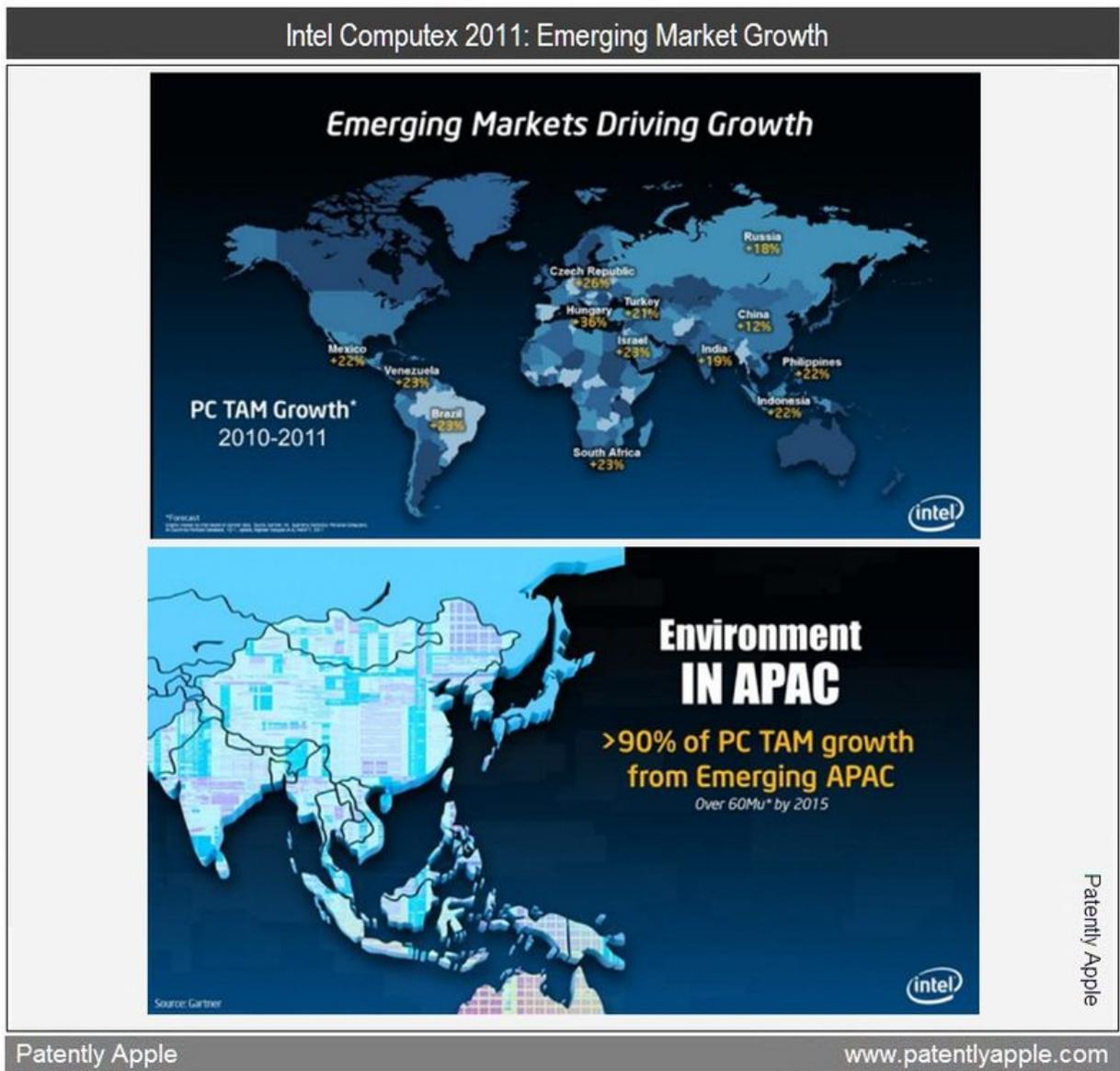
Intel, Apple & the Transformation of the PC

Like most Intel keynotes, they begin with charts, facts and figures that will form the foundation of their presentations. Two out of the three presentations at Computex 2011 began with a series of presentation slides on where future PC growth will be coming from over the next decade.

According to Mooly Eden, Corporate Vice President and GM of PC Client Group, two out of every three PC's sold next year will be attributed to Emerging Market Growth. Two out of three PC's will be notebooks and two out of three PC's will be sold to consumers.

As you could see below, there's an Intel slide illustrating the Total Amount of Market (TAM) Growth in various areas of the world. Interestingly, according to Eden, America will fall to number two next year with the People's Republic of China, or PRC, finally taking over as the leader in PC growth. Brazil will be number three.

Intel, Apple & the Transformation of the PC

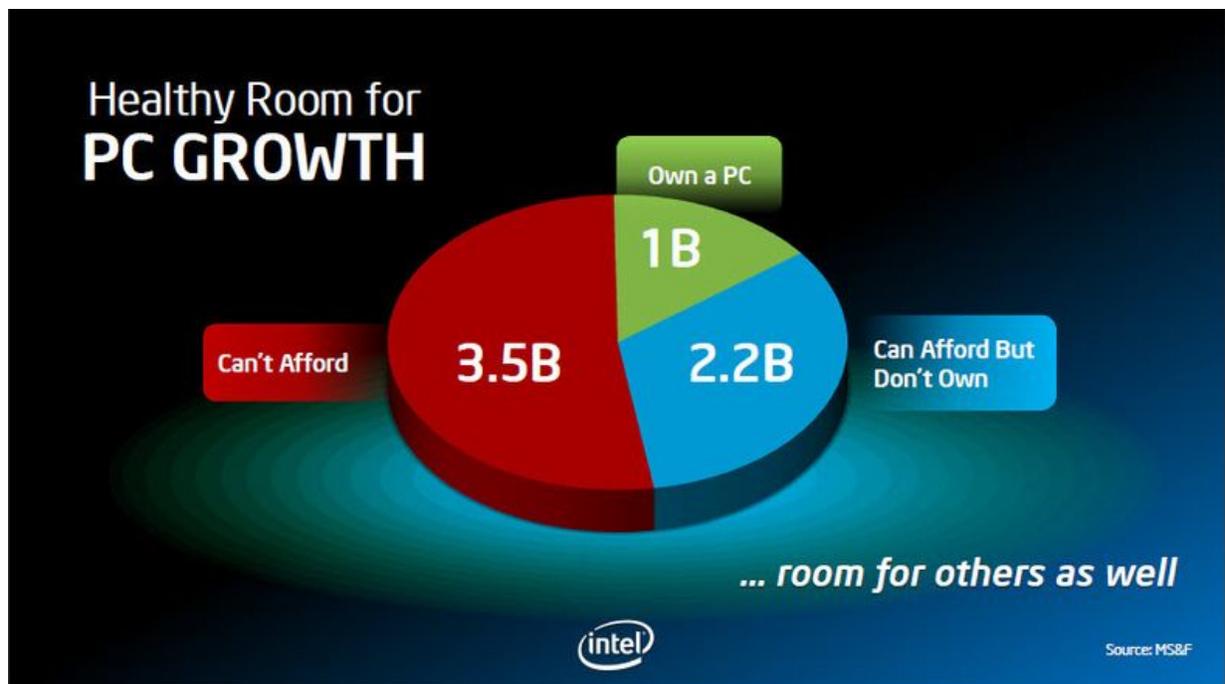


To break those figures down even further, Eden stated that the growth coming from Asia Pacific (APAC) wasn't coming from countries that you'd think, like Australia, New Zealand or even Taiwan. The real growth was going to come from countries like India, the Philippines, Malaysia and Indonesia.

Intel's Vice President Sean Maloney brought another interesting fact to the table. He stated that by 2016, there will be over two billion PC users – doubling today's PC base. The affordability gap keeps another 3.5 billion out of the market. Closing the

Intel, Apple & the Transformation of the PC

affordability gap is one the smartest strategy the industry can pursue, stated Maloney.



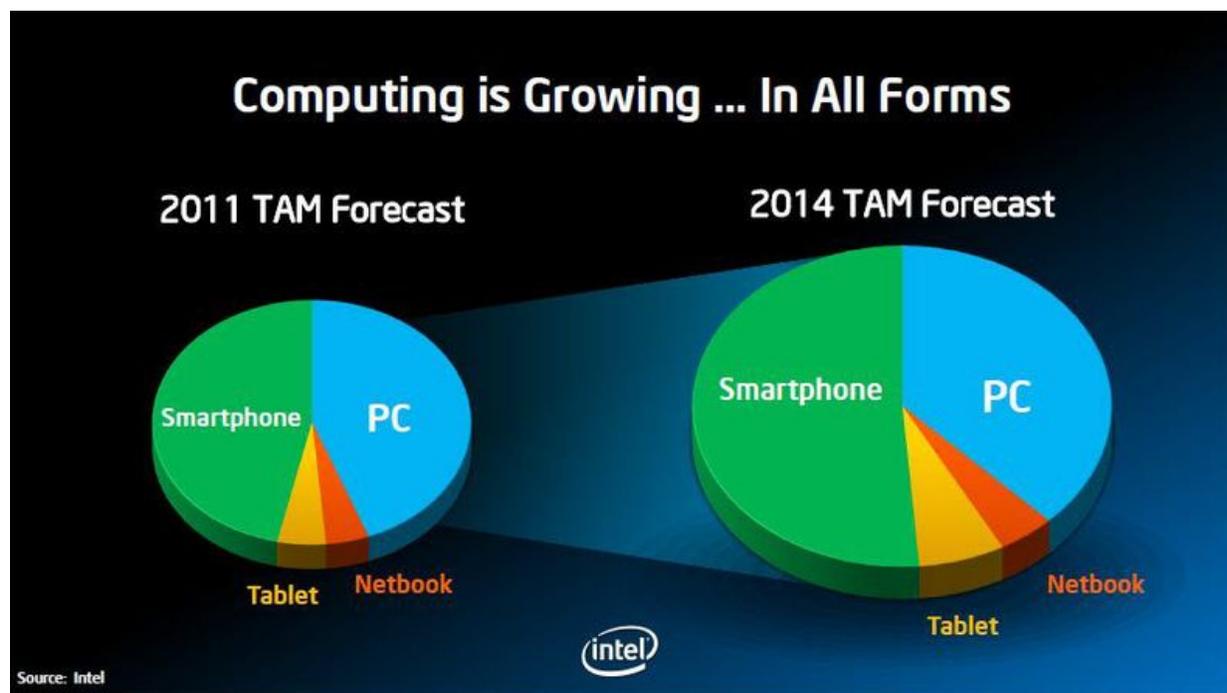
So in perspective, Tim Cook's commentary about tablets eclipsing the PC market is likely focused on traditional markets as opposed to the global market which still has enormous headroom for growth. The two clashing visions of the PC industry therefore are simply stemming from differing positions in the market. Steve Jobs stated back in 1996 that Apple lost the PC war long ago and so their indifference to its future is understandable – yet obviously skewed.

Think Computing, Not PC

From Intel's perspective, as indicated by their next slide, the thought of tablets eclipsing the PC market over the next several years just doesn't compute – unless Apple is trying to clump tablets in with smartphones under one gigantic "tablet" category. But that would be a marketing shell game and the stats below focus on computing in the four main categories as recognized by all analysts in the market: Smartphones, Personal Computers, Tablets and Netbooks.

Intel, Apple & the Transformation of the PC

In the bigger picture, Intel's focus is shifting from thinking and talking PCs to thinking and talking Computing. That honestly began back in 2009 when Otellini introduced the concept of "[Building a Continuum of Computing](#)." So while the press likes to overly play up the decline of the PC, it's really an old argument and an over simplification of what's really happening in computing in general.



Intel's 2011 chart shows tablets and netbooks being neck to neck at the moment and tablets getting the upper hand by 2014. Why 2014? Because that gives Intel time to get into that race which plays nicely into their version of the marketing shell game. Intel being "the source" of that data is of course suspect to say the least. Yet with that said – Computex 2011 was all about loudly banging the drum to announce that change was coming to both the netbook and Personal Computer: Huge change.

In 2010, Canals Vice President and [Principal Analyst Chris Jones](#) stated that "Apart from the 'Apple effect', the iPad owes its success to a lack of advancement in other portable computing segments, such as netbooks." I think that Intel has heard this common complaint loud and clear as they tried to address this urgency for change.

Intel, Apple & the Transformation of the PC

Intel's Maloney stated that coming Medfield processors will power tablets and smartphones in 2012. They're being evaluated by Intel's customers at this very moment and will ship sometime between mid Q4 2011 and Q1 2012. The new Atom processors will provide better battery life, superfast computing, ultimate gaming and Advanced Imaging which copied Apple's [Retina](#) marketing imagery of the eye. On the tablet and smartphone front, Intel failed to impress once again.



The image is a promotional slide for the Intel Medfield processor. At the top, the word "Medfield" is written in a large, white, sans-serif font. Below this, there are four columns, each with a feature name and a corresponding image. The first column is "Long Use Time" with an image of several blue cylindrical batteries. The second is "Super-Fast Computing" with an image of a car's dashboard and steering wheel. The third is "Ultimate Gaming and Media" with an image of a character from a video game. The fourth is "Advanced Imaging" with an image of a human eye with a rainbow-colored iris. Below these four columns, there is a dark blue banner with white text that reads: "First 32 nm Smartphone and Tablet Platform", "Tablet reference design enabling sub 9mm designs that weigh less than 1.5 lbs.", and "Product shipping in the next 6-9 months". At the bottom center of the slide is the Intel logo.

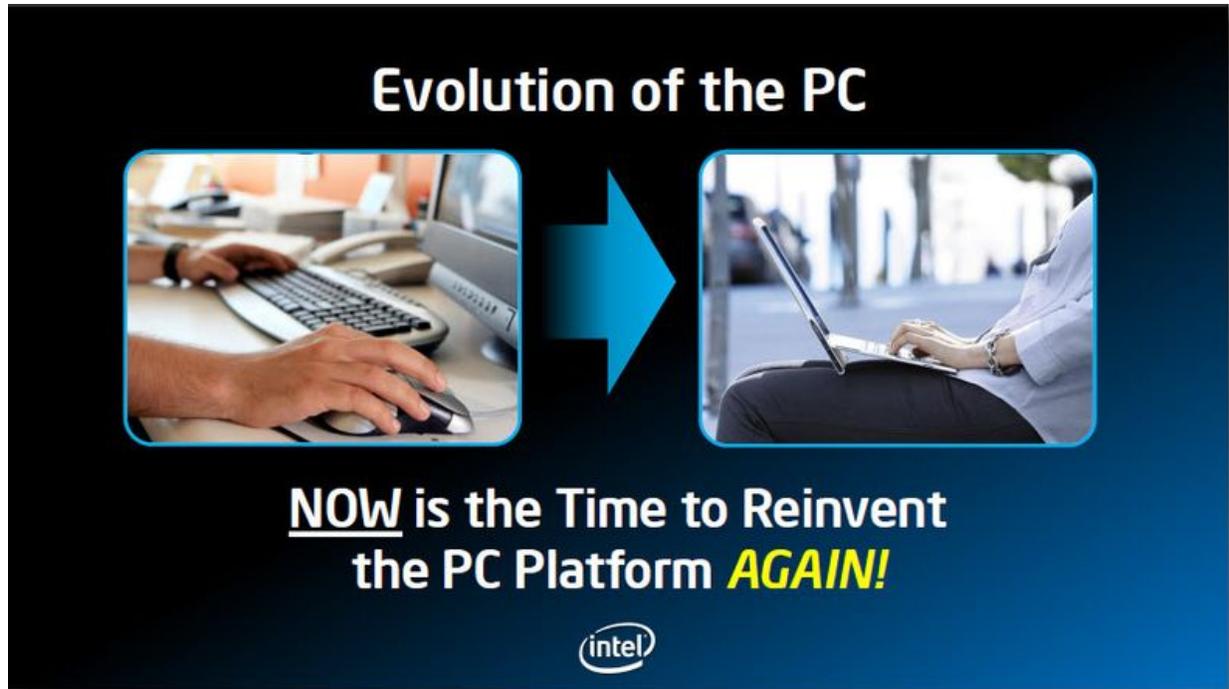
But the real story was in Intel's main message of change to the Personal Computer.

Huge Changes are Coming to the Personal Computer

In Sean Maloney's keynote, he stated that "the PC must continue to evolve. Consumers are demanding new experiences and the PC has to be able to meet those demands. Simply put, the PC must undergo a major change – Again! Think back to the shift from the desktop centric computing model to the introduction of Centrino and mobility in 2003: That kind of change. So how do we do that? We do that from the

Intel, Apple & the Transformation of the PC

inside out. How it looks, how it feels, how the user experiences it."

A graphic titled "Evolution of the PC" on a dark blue background. It features two square images with blue borders. The left image shows a person's hands typing on a desktop keyboard and using a mouse. A large blue arrow points from this image to the right image, which shows a person sitting and using a laptop. Below the images, the text reads "NOW is the Time to Reinvent the PC Platform **AGAIN!**" in white and yellow. The Intel logo is centered at the bottom of the graphic.

Evolution of the PC

NOW is the Time to Reinvent
the PC Platform **AGAIN!**

intel

Intel Introduces Smart Connect, Rapid Start & Smart Response Technologies

The first two new technologies coming to market soon are Smart Connect and Rapid Start. The latter takes the system and application states and puts them onto a dedicated Flash Drive which uses no power. To make that point, the demonstrator pulled the battery out of a notebook and then reinstated it. After opening the lid of the notebook, it only took 6 seconds to wake up without a reboot which you'd have to do if you removed the battery from a notebook today. There was a lot of applause for that announcement.

Intel, Apple & the Transformation of the PC

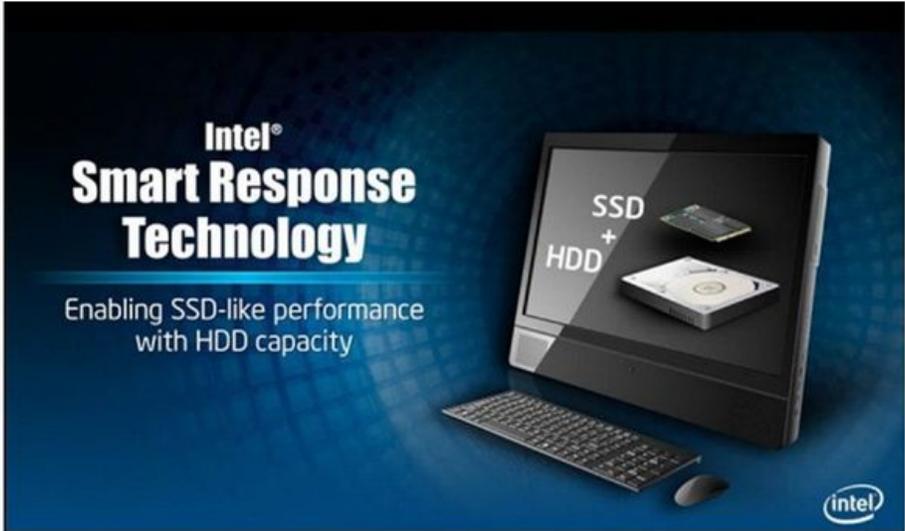
The advertisement features a dark blue background. In the top left, a blue box contains the text 'Intel® Smart Connect Technology' and 'Content continuously updated while the notebook is asleep!'. To the right is an illustration of a closed laptop with several colorful social media icons (email, Twitter, Facebook, RSS, etc.) floating above it. In the bottom left, a graphic shows a globe on top of a laptop keyboard, with the words 'ALWAYS ON' and 'ALWAYS ON' arranged around it. In the bottom right, a blue box contains the text 'Intel® Rapid Start Technology' and '~5-6 seconds from hibernate!'. The Intel logo is centered at the bottom.

The third new technology on its way this fall is called Smart Response Technology which enables SSD-like performance with HDD capacity. In a nutshell, Eden stated that what they've done is combined the goodness of both by combining a very big hard drive complimented with 20 or 40 Gig of cache and make sure that the whole system appears to be running as if it was a solid state drive.

In terms of raw speed, Eden compared the differences between a pure SSD to an HDD and then to Intel's new smart response technology based drive-system. The times for a particular task came in respectively at 33 seconds for SDD, 58 seconds for the HDD and 34 second for Intel's Smart Response Technology based drive system. If we're to believe Intel's test results, then we could be in store for snappier drives on Macs this fall.

Intel, Apple & the Transformation of the PC

Intel's Smart Response Technology SSD + HDD



Intel®
**Smart Response
Technology**

Enabling SSD-like performance
with HDD capacity

SSD
+
HDD

Patently Apple

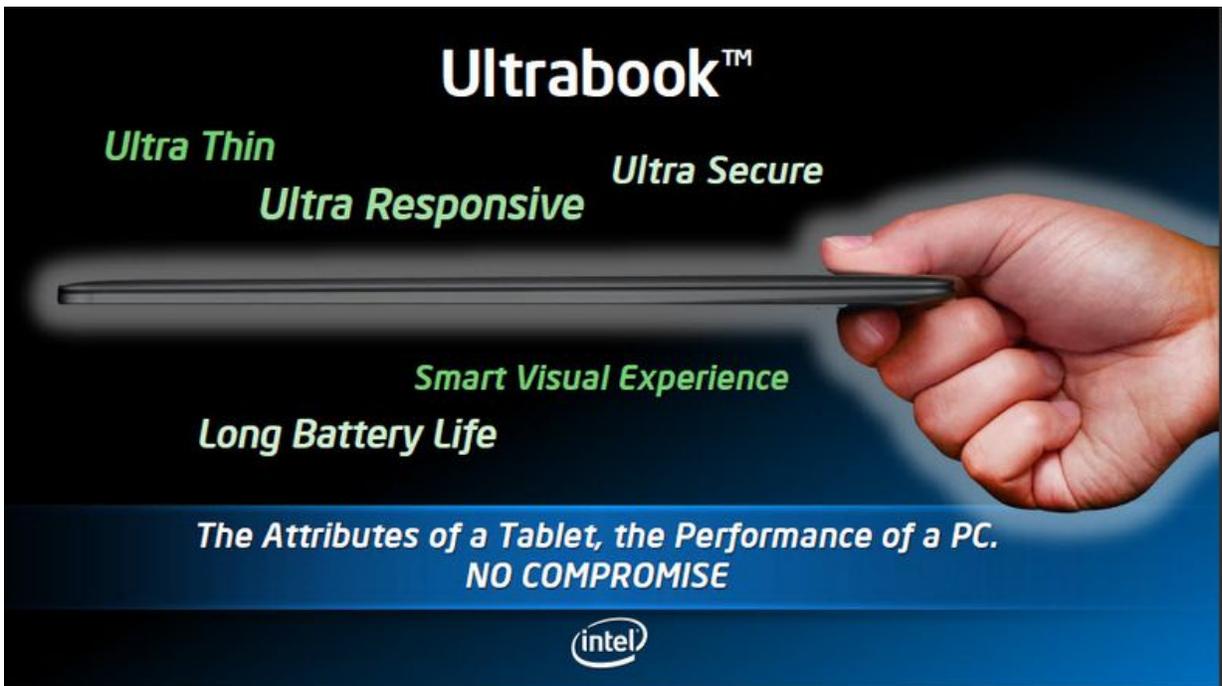
Patently Apple www.patentlyapple.com

The advertisement features a dark blue background with a grid pattern. On the left, the text 'Intel® Smart Response Technology' is prominently displayed in white, with 'Enabling SSD-like performance with HDD capacity' below it. On the right, a laptop is shown with a keyboard and mouse. The laptop screen displays 'SSD + HDD' and images of an SSD and an HDD. The Intel logo is in the bottom right corner of the image area. Below the image, the text 'Patently Apple' is centered. At the bottom of the slide, 'Patently Apple' and 'www.patentlyapple.com' are displayed on the left and right respectively.

Intel Introduces Ultrabook

The three new features previously outlined will be at the heart of Intel's new Ultrabook category – which is a no compromise version of what the notebook could be. Intel boldly believes that the Ultrabook will represent 40% of the consumer market by the end of 2012.

Intel, Apple & the Transformation of the PC

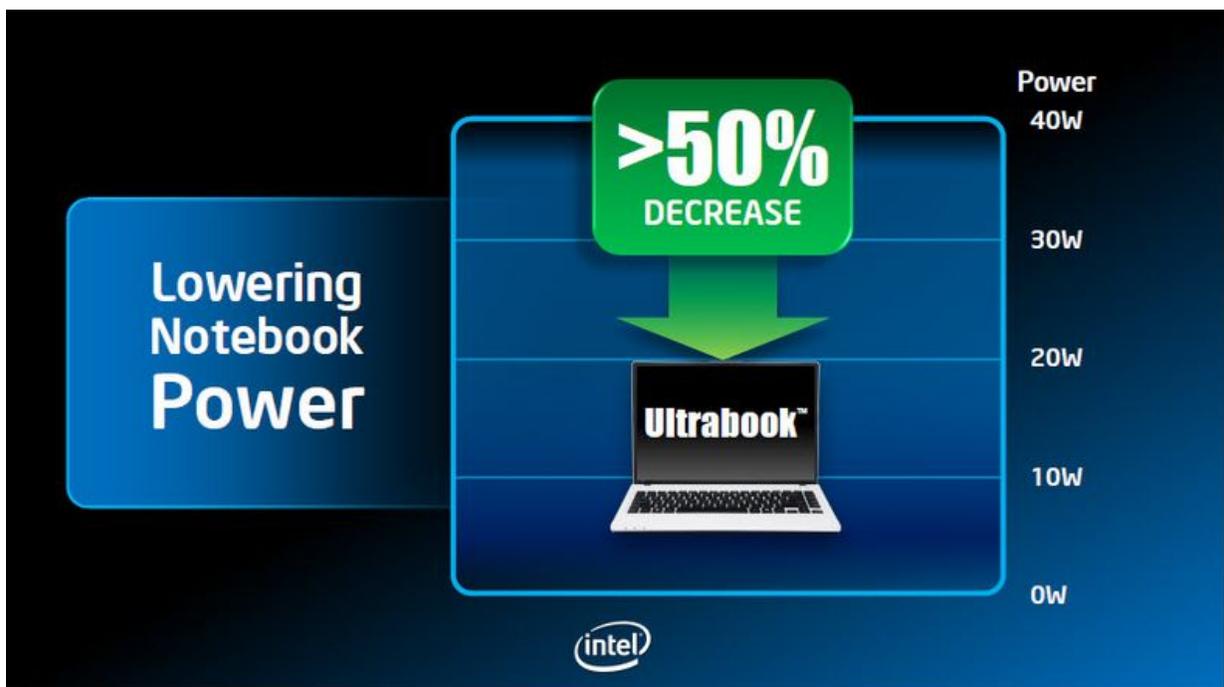


Intel stated that their Ultrabook platform will enable a new user experience by accelerating a new class of mobile computers. These PCs will marry the performance and capabilities of today's laptops with tablet-like features and deliver a highly responsive and secure experience in a thin, light and elegant design that will include USB 3.0 and Thunderbolt.

Intel, Apple & the Transformation of the PC



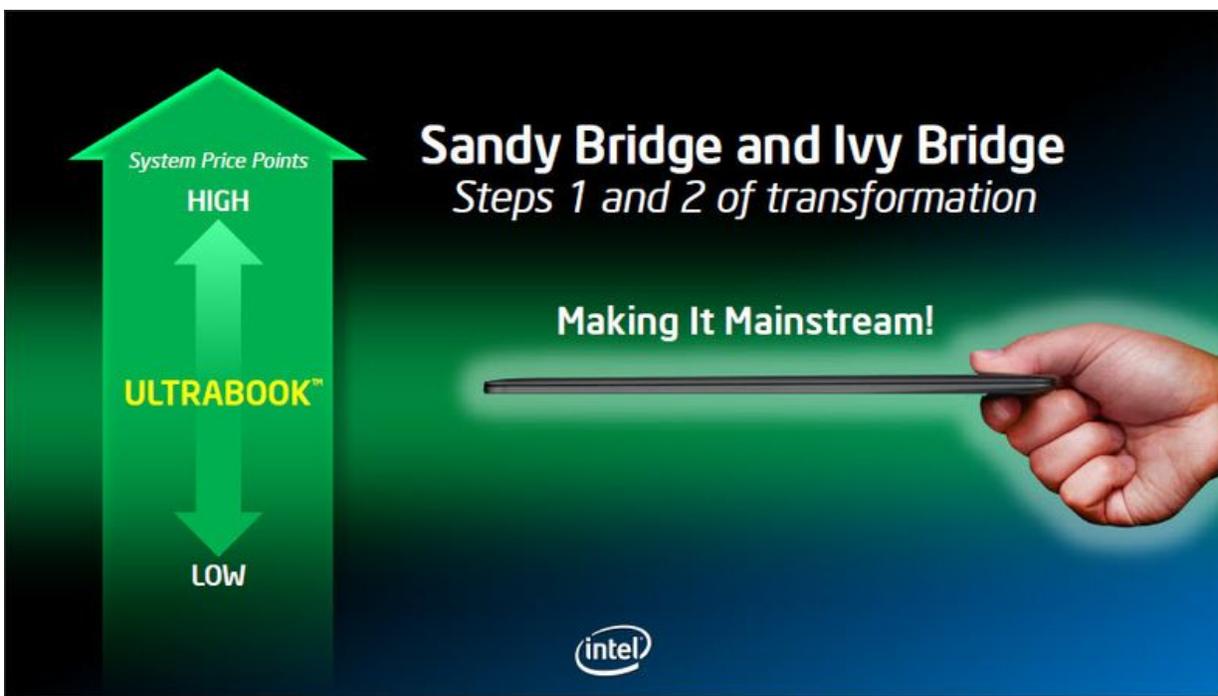
The unit that Intel kept pushing on stage that is to embody the initial Ultrabook features was the Asus UX21 – which is really a copycat of Apple's MacBook.



Intel, Apple & the Transformation of the PC

Intel's Ivy Bridge Will Be an Unusual Leap Forward

The next evolution is just around the corner. With new advances coming to Sandy Bridge this fall being considered step one of reinventing the PC, Intel's Ivy Bridge represents step two. Intel's coming Ivy Bridge is built on their industry leading 22 nanometer process. It will bring power efficiency to the notebook PC and unrivaled security for consumers: identity theft protection, better encryption and automatic malware detection.



Interestingly, Ivy Bridge, according to Intel's roadmap, was to be a classic "Tick" in their famous Tick-Tock model. But according to Intel's Eden, "Ivy Bridge is going to be a big "Tick +" because in order to make sure that we could deliver the right user experience we decided to take a risk and implement architectural changes inside Ivy Bridge. And for that reason when you see Ivy Bridge, many of you will be surprised." In affect Intel is squeezing a two year cycle into one so as to accelerate the PCs transformation into something more appealing.

Intel, Apple & the Transformation of the PC

Intel, Apple & the Transformation of the PC

Intel Accelerates Their Roadmap: Ivy Bridge Will be an Architectural & Processor Shift

NEWEST MANUFACTURING TECHNOLOGY DELIVERS IVY BRIDGE

45 nm Process Technology		32 nm Process Technology		22 nm Process Technology
Penryn	Nehalem	Westmere	Sandy Bridge	Ivy Bridge
TICK	TOCK	TICK	TOCK	TICK+
				Intel's First 22 nm Processor



22 nm 3-D Tri-Gate Transistor

The Foundation for All Computing

Process Technology Leadership

2003	2005	2007	2009	2011
90 nm	65 nm	45 nm	32 nm	22 nm
Inverted SGate Strained Silicon	2nd Gen SGate Strained Silicon	Inverted Gate Last High-K Metal Gate	2nd Gen Gate Last High-K Metal Gate	3rd Gen Inverted Tri-Gate

Transistors have now entered the third dimension!

22nm

A Revolutionary Leap in Process Technology

- 37%** Performance Gain at Low Voltage*
- >50%** Active Power Reduction at Constant Performance*

Source: Intel
*Compared to Intel 32nm Technology

2012 – IVY BRIDGE

Smart Performance and Responsiveness	Seamless Visual Experience	Security for Consumers
<ul style="list-style-type: none"> • Longer Battery Life • Better Performance • Always-on/Always Connected, and More Responsive • Integrated USB3 • Thunderbolt 	<ul style="list-style-type: none"> • Better Transcode HD-HD • HD Video Conferencing • Improved Graphics Performance and DX11 support 	<ul style="list-style-type: none"> • Better Identity Protection • Better Encryption • Increased Malware Protection



Patently Apple

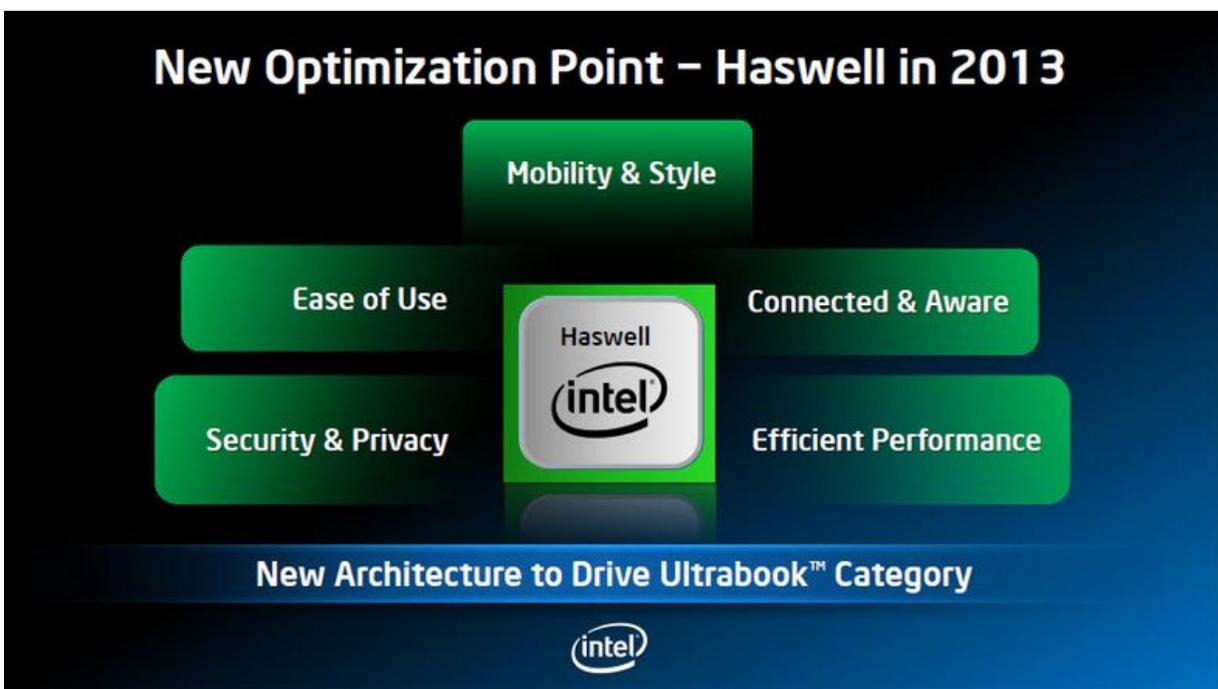
Patently Apple www.patentlyapple.com

Intel, Apple & the Transformation of the PC

One of the key points that Eden tried to stress in his presentation was that Ivy Bridge's architecture would allow OEMs to custom design many kinds of devices with the one architecture. In respect to notebooks, the craze to go Ultra thin means that some snappiness could be lost if you're trying to do high end work. Yet for those wanting a snappy on-the-go system for simple apps like email, surfing, playing music and so forth, the new Ivy Architecture will rock. And if you need to edit photos, do some transcoding or play a game at home, you'll be able to ramp up the performance of your notebook with the assistance of next generation docking station solutions that will provide superior cooling systems.

Intel's 2013 Haswell Processor Changes Everything!

So why is Intel ramping up Ivy Bridge to be way ahead of schedule and include a new microarchitecture? Because Intel is rushing their new from scratch processor called Haswell for 2013 in an effort to take on ARM and any other wannabe competitor in the mobile space.



Intel, Apple & the Transformation of the PC

Perhaps Intel's marketing department should have dubbed this new processor Roswell instead of Haswell – because the way that Intel's Eden was promoting it sounds like it could be from out of this world. According to Intel's Eden, Haswell is going to be totally different platform from top to bottom. It's going to be a totally different architecture.

Intel's Big Surprise: Haswell. A Totally Different Platform. A Totally Different Architecture

THE 2013 ULTRABOOK™ PC
It's a tablet when I want it.
It's a PC when I need it.
All day. Every day.

It is an expression of me
I like the way it looks
I get back to what I was doing instantly
It responds to my voice or a wave of my hand...
I'm on Facebook instantly
It knows me, my phone, where I am...
It protects me and my stuff...
And it never keeps me waiting.

All Day Battery Life **Best-In-Class Performance**
Instant On **Runs Multiple Operating Systems** **Mainstream Price Points**
Touch Interface **Seamless Interconnectivity Between Devices** **Best-In-Class Graphics**
Always Connected **Security**

Patently Apple

Patently Apple www.patentlyapple.com

Intel, Apple & the Transformation of the PC

Evolution vs. Revolution

At the end of the day, two out of three Intel keynotes coming out of Computex 2011 this week focused on accelerating advances in the PC so as to generate more excitement for the PC sector in light of popular consumer devices like Apple's iPad. In the short term, Intel will jazz up Sandy Bridge processors for this fall and then deliver a wild leap in PC power in 2012 with their 22nm Ivy Bridge platform with USB 3.0, Thunderbolt, advanced security, cooler thermals promoting ultrathin designs and much-much more.

Yet Intel knew that the advances coming to Ivy Bridge wouldn't be enough to satisfy their developers or the media's desire to hear how they intend to respond to Apple's never-ending freight train run of innovation. So they uncustomarily opened up their 2013 roadmap to reveal an all new from scratch processor dubbed Haswell: It'll power a tablet when you want it; be a PC when you need it and provide you with an all-day battery. It almost sounded revolutionary and that's what Intel wanted to hang their hat on this week in Taiwan.

The only real problem with Intel's revelations is that many of their innovations will be left in the dust after Steve Jobs' keynote on Monday. Apple will finally take the wraps off their upgraded operating systems and reveal their all-new iCloud music service.

In the fall, Apple will deliver yet another new stream of advances to keep Intel and their developers up at night and it's this never ending cycle that is driving the traditional PC industry mad. Innovation is the engine to the mobile revolution and while Google's Android and HP's WebOS will make inroads this year no doubt, Apple's innovation and power to step on the gas on a moments-notice is what keeps Apple at the forefront of this revolution.

Tomorrow, we'll celebrate true innovation, again.

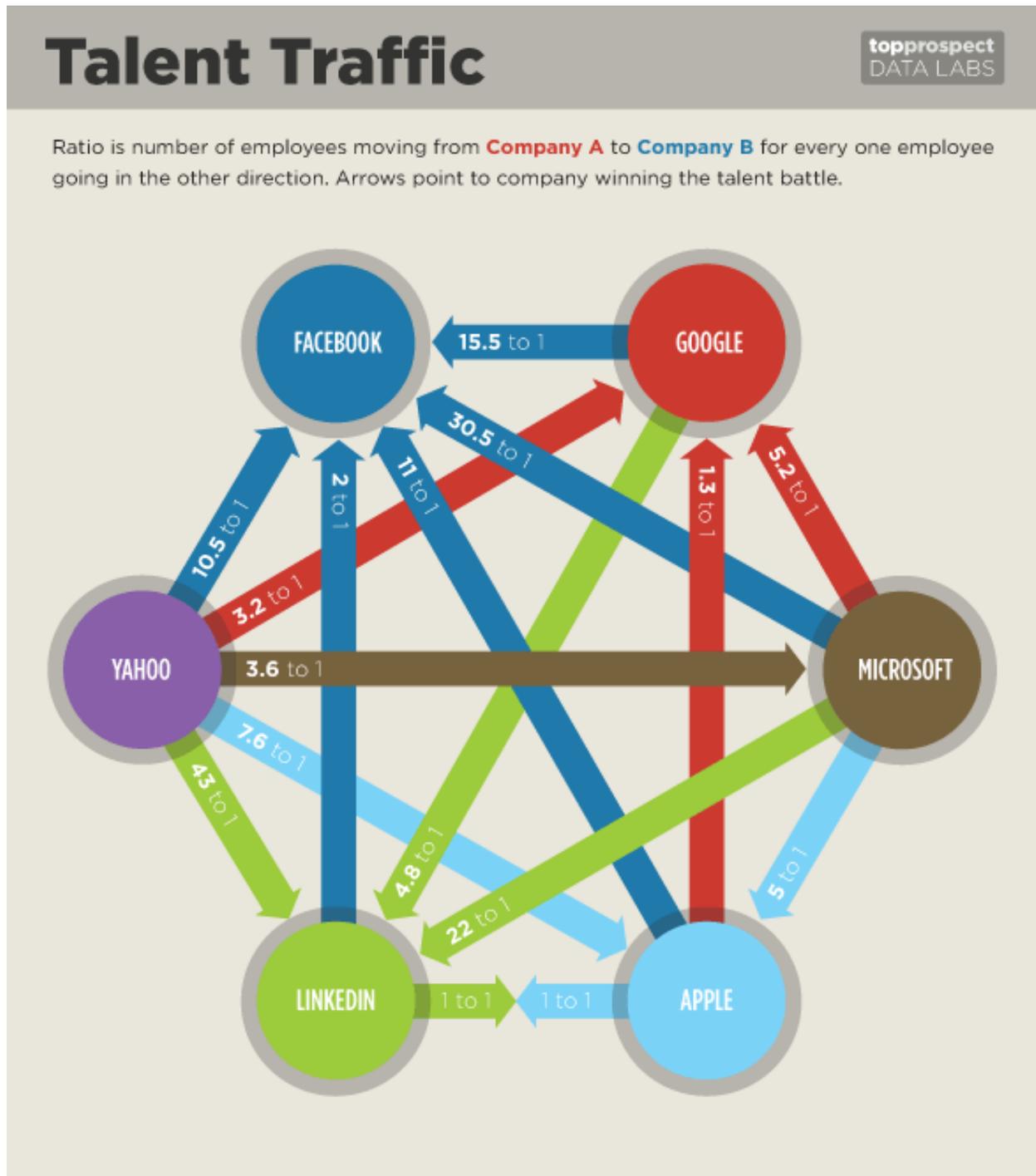
Which Hot Tech Companies Are Winning the Fight for Top Coders?

Which Hot Tech Companies Are Winning the Fight for Top Coders?

•

- By [Ryan Singel](#)   June 7, 2011 | 4:28 pm | Categories: [Corporate](#), [Silicon Valley](#) [@rsingel](#) · 2,154 followers

Which Hot Tech Companies Are Winning the Fight for Top Coders?



The battle for top sales people and engineers is extraordinary in Silicon Valley and New York City — even if the employment numbers in the rest of the country remain

Which Hot Tech Companies Are Winning the Fight for Top Coders?

anemic.

Job boards are everywhere these days; tech companies are paying tens of thousands in signing bonuses and even more to keep key employees; and tech companies are having to spend millions to buy small startups just to get their engineering talent.

But who is winning the battle?

[TopProspect](#), a crowd-sourced headhunting startup based in San Francisco that pays users a minimum of \$6,000 if they successfully refer a friend to a job, thinks they know. They [ran the numbers on their members](#) and their contacts to see who had switched jobs in the last two years.

The big winners?

Well, if you look at the number of people who left compared to the number who joined, you can see the power of stock options at hot companies.

Twitter hired nearly 11 employees for every one lost; Facebook and Zynga averaged about eight new hires for every defection, while LinkedIn clocked in at +7.5 and Groupon at +3.9. Other big names fared less well: Intuit hired 1.2 for every one lost, the same ratio as Google. Meanwhile others are bleeding talent: eBay hired 0.8 people for every person who left, Microsoft got just 0.4 and Yahoo 0.3 (not surprising, given Yahoo laid off hundreds at Christmas time.)

In terms of raw numbers of new employees, Google, Facebook, Microsoft, LinkedIn and Apple were tops — not surprising given their size. But some of those same companies were also on the list of the top five biggest losers: Microsoft, Yahoo!, Google, eBay, and Amazon.

Which Hot Tech Companies Are Winning the Fight for Top Coders?

As for the data set, Top Prospect says it covers its user base and their networks, which comes out to about 2.5 million profiles, that are largely Bay Area-focused. So while it's no census, it's a pretty good snapshot of the tech industry.

Happy IPv6 Day

June 8, 2011, 8:58 AM

Happy IPv6 Day

By [VERNE G. KOPYTOFF](#)

Get out the confetti. Wednesday is [World IPv6 Day](#).

If you are unaware of the event, you're hardly alone. Few people know about it and if it is a success, it should stay that way.

The day nevertheless marks an important step in the Internet's evolution. The event is intended as a "test flight" for a successor to the current Web address system that – if successful – will help to ensure that the Internet runs smoothly into the future.

IPv6, as the Web address system is known, is intended to relieve the strain on a system that has been used since the Internet's inception. IPv4, the original address system, was devised without consideration for how big the Internet would eventually become as a means for buying diapers, downloading music and sending risqué photos.

The problem is that IPv4 addresses are nearly all taken. The last batches were made available in February and are expected to be claimed by the end of the year.

The addresses are not the Yahoo.com, Facebook.com and Google.com that nearly everyone recognizes. Rather, they are the basic numeric addresses that those domains stand-in for.

IPv4 addresses consist of 32 zeros and ones in different sequences. There are roughly 4.3 billion such addresses.

IPv6 addresses consist of 128 numbers. Given all the possible combinations of zeros and ones, the system offers around 320 [undecillion](#) numbers.

Leslie Daigle, chief technology officer for the Internet Society, a nonprofit group that is promoting World IPv6 Day, put it this way: There are more IPv6 addresses "than there

Happy IPv6 Day

are grains of sand on Earth.”

On Wednesday, more than 400 Web content [companies like Google](#), Yahoo and [Facebook will participate](#) in World IPv6 Day by making their sites accessible over IPv6. The goal is to motivate organizations across the Internet industry to prepare their services for IPv6.

People who are curious about whether their Internet connections are IPv6-ready can [test them](#).

The change will likely go unnoticed by most everyone. However, a small percentage of Internet users – less than half a percent, according to the Internet Society – may notice a temporary slowdown because of incorrectly configured equipment, particularly home networking equipment.

In reality, most of the preparation has already been done by backbone Internet providers, Internet service providers, Web sites and Web site hosting services.

The alternative to the transition to IPv6 is far worse than any minor glitches for a fraction of the Internet using population. The Internet would become increasingly slow for everyone and more costly for Internet companies to do business because they would have to spend money on working around the problem, Ms. Daigle said.

“Your games don’t work, or your Google Maps doesn’t fill in as smoothly as before,” she offered as examples.

IPv6 addresses have been available for years. But they represent only a fraction of all addresses, although that will undoubtedly change in coming years.

Google, Microsoft, and Yahoo Team Up to Advance Semantic Web

Friday, June 10, 2011

Google, Microsoft, and Yahoo Team Up to Advance Semantic Web

A push to add meaning to Web pages to aid search could also enable other kinds of intelligent web apps.

By Tom Simonite

Google, Microsoft, and Yahoo have teamed up to encourage Web page operators to make the meaning of their pages understandable to search engines.

The move may finally encourage widespread use of technology that makes online information as comprehensible to computers as it is to humans. If the effort works, the result will be not only better search results, but also a wave of other intelligent apps and services able to understand online information almost as well as we do.

The three big Web companies launched the initiative, known as [Schema.org](#), last week. It defines an interconnected vocabulary of terms that can be added to the HTML markup of a Web page to communicate the meaning of concepts on the page. A location referred to in text could be defined as a courthouse, which Schema.org understands as being a specific type of government building. People and events can also be defined, as can attributes like distance, mass, or duration. This data will allow search engines to better understand how useful a page may be for a given search query—for example, by making it clear that a page is about the headquarters of the U.S. Department of Defense, not five-sided regular shapes.

The move represents a major advance in a campaign initiated in 2001 by Tim Berners-Lee, the inventor of the Web, to enable software to access the meaning of online content—a vision known as the "semantic Web." Although the technology to do so exists, progress has been slow because there have been few reasons for Web page operators to add the extra markup.

Schema.org may change that, says [Dennis McCleod](#), who works on semantic Web technology at the University of Southern California. By tagging information, Web page owners could improve the position of their site in search results—an important source of traffic. "This will motivate people to actually add semantic data to their pages," says McCleod. "It's always hard to predict what will be adopted, but generally, unless there's something in it for people, they won't do it. Google, Microsoft, and Yahoo have given people a strong reason."

The Schema.org approach is modeled on one of the more straightforward methods of

Google, Microsoft, and Yahoo Team Up to Advance Semantic Web

describing the meaning of a Web page's contents. "The trouble with many of these techniques is, they are really hard to use," says McCleod. "One of the encouraging things about Schema.org is that they are pursuing this at a level that is quite usable, so it is much easier to mark up your website."

If many Web page owners act on Schema.org's suggestions, more than just search will benefit. "This data can be used by any software to cross-correlate things that are related, or to understand the relationship between information from different sources," says McCleod. For example, widespread availability of semantic information might improve artificially intelligent assistants, such as Siri (bought last year by Apple). Or tools able to make good recommendations of, say, news articles because they can know for sure what stories are referring to.

However, the companies behind Schema.org made their move unilaterally, without consulting the World Wide Web consortium (W3C), the standards body for Web technology. "We had no idea this was coming," says Manu Sporny, a member of the W3C's Semantic Web Coordination Group.

Schema.org asks for semantic markup to be written using a format known as microdata, which is not yet a W3C standard, rather than RDFa, a more widely used W3C-approved alternative.

Google has warned that its "crawlers" that roam the Web to build its index could be confused by a page using both microdata and RDFa. Yet Microsoft has previously said its own crawlers have no such problems, says Sporny.

If that confusion isn't straightened out, he says, microdata may become the only standard used at any scale, which would limit the power of the semantic Web, because the alternative can do much more. "RDFa supports use cases that microdata can't—for example, the WHO publishing mortality rates for different countries or adding semantic information to eBook or image files," he says.

Sporny hopes that Google and others behind Schema.org will modify their stance on formats. But he acknowledges that having such large companies embrace the semantic approach is a good thing. "They are saying you will get better results with semantic Web concepts," says Sporny, "and if they encourage more sites to embrace the semantic Web, that will help all kinds of other applications, too."

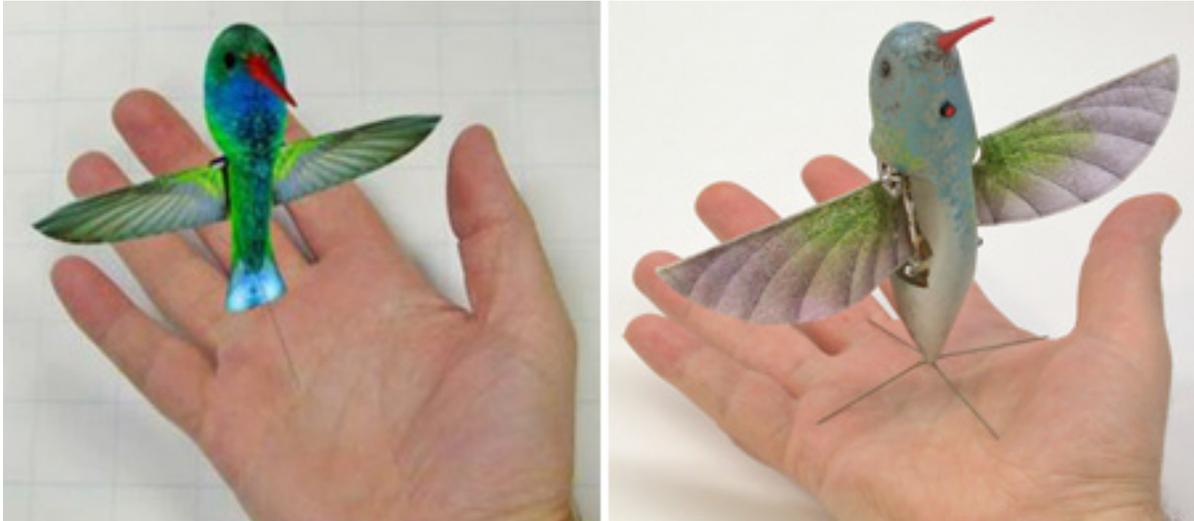
Copyright Technology Review 2011.

Google, Microsoft, and Yahoo Team Up to Advance Semantic Web

DARPA Concludes Nano Air Vehicle Program, We Wonder What's Next

DARPA Concludes Nano Air Vehicle Program, We Wonder What's Next

POSTED BY: EVAN ACKERMAN / WED, JUNE 01, 2011



The original concept, on left, and the final robot, on right

We've written a fair number of articles starting with the phrase "DARPA wants" followed by something that's nearly always entirely improbable and often borderline nutty. It's rare that DARPA actually *gets* exactly what it wants, but with their Nano Air Vehicle program, that seems to have happened.

As the above video shows, it was definitely not an easy process to make a life sized, fully controllable surveillance robot that's more or less indistinguishable for a hummingbird, but AeroVironment managed to pull it off. Of the technical goals and milestones that DARPA set out for the robot, it managed to meet all and exceed many:

- Demonstrate precision hover flight within a virtual two-meter diameter sphere for one minute.
- Demonstrate hover stability in a wind gust flight which required the aircraft to hover and tolerate a two-meter per second (five miles per hour) wind gust from the side, without drifting downwind more than one meter.
- Demonstrate a continuous hover endurance of eight minutes with no external power source.
- Fly and demonstrate controlled, transition flight from hover to 11 miles per hour

DARPA Concludes Nano Air Vehicle Program, We Wonder What's Next

fast forward flight and back to hover flight.

- Demonstrate flying from outdoors to indoors, and back outdoors through a normal-size doorway.
- Demonstrate flying indoors 'heads-down' where the pilot operates the aircraft only looking at the live video image stream from the aircraft, without looking at or hearing the aircraft directly.
- Fly the aircraft in hover and fast forward flight with bird-shaped body and bird-shaped wings.

AeroVironment says that it would take a decade to make this robot ready for deployment, but DARPA doesn't just hand out piles of cash to make cool stuff for no reason. There's a future here, whether or not we hear about it immediately, so just make sure to give hummingbirds a second look from now on.

[[Nano Air Vehicle Program](#) and [AeroVironment](#)]

Pentagon's Drone Surge Includes \$5.3 Billion for General Atomics

Bloomberg Government (bgov.com)
May 31, 2011

Pentagon's Drone Surge Includes \$5.3 Billion For General Atomics

By Brendan McGarry, Bloomberg News

The number of aerial drones with combined strike and surveillance capabilities, such as General Atomics' Reaper, will more than triple over the next decade, according to the U.S. Defense Department's 2011 Aircraft Procurement Plan.

The demand for unmanned systems, which offer expanding abilities without risk to human pilots and at generally lower cost, will create business opportunities for suppliers such as General Atomics of San Diego and FLIR Systems Inc. of Wilsonville, Oregon, even as Congress aims to trim the defense budget amid trillion-dollar deficits.

"It's certainly a huge growth area," Mark Gunzinger, a senior fellow at the Center for Strategic and Budgetary Assessments, a research organization in Washington, said in a telephone interview. "We really are at the front end of understanding what unmanned vehicles -- not just air, but undersea and land -- can do for us operationally, and what it's going to lead to in terms of changes to our industrial base."

The Reaper, big brother to the Predator, also made General Atomics, is called a "hunter-killer" for its ability to soar up to 50,000 feet, loiter for hours and pound targets with air-to-ground missiles and laser- and GPS-guided bombs.

The Pentagon plans to increase its stock of Reapers and other "unmanned, multirole, surveillance and light-strike" unmanned aircraft to 536 in 2021 from 140 in fiscal 2012. Overall, the number of medium- and high-altitude drones will climb to about 728.

The Pentagon plans to spend \$259 billion on aircraft development and procurement through fiscal 2021. Investments would peak at \$30 billion in fiscal 2016. It's unclear how much of that would go to drones.

The Predator, workhorse of the wars in Iraq, Afghanistan and, more recently, Libya, will be phased out over the next decade, according to the Pentagon forecast. The Reaper will play a larger role in its place, as will other as-yet-undeveloped systems, including a stealth drone designed to operate from aircraft carriers.

Drones are slated to replace the Cold War-era U-2 spy plane sometime after fiscal 2016, and possibly the RC-135 Rivet Joint surveillance plane and the E-3 Sentry, an airborne warning and

Pentagon's Drone Surge Includes \$5.3 Billion for General Atomics

control system, over the next few decades, according to the Defense Department report.

“We’re clearly hitting the next stage in the history of a new weapons class introduction,” Peter W. Singer, a senior foreign policy fellow at the Brookings Institution and the author of the book, “Wired for War,” said in a telephone interview. “The first stage is this battle to prove that it’s worthwhile, that it can be useful. The second stage is when it begins to proliferate out into a number of other areas that it wasn’t originally designed for. That’s what we’re entering.”

The U.S. military has more than 7,000 unmanned aerial vehicles, or UAVs, up from just a handful a decade ago, Singer said. The vast majority are small, low-altitude systems, often no bigger than model airplanes flown by hobbyists, designed to improve surveillance for ground troops looking for the enemy nearby. The bigger systems, including the RQ-4 Global Hawk, made by Los Angeles-based Northrop Grumman Corp., and General Atomics’ MQ-9 Reaper and MQ-1 Predator, survey large swaths of territory. Lower Cost

Sensors on the drones allow operators to identify smaller targets, such as people, Dyke Weatherington, deputy director for unmanned warfare at the Pentagon, said in an e-mail. They do it while offering potentially lower operating costs than manned aircraft, little to no risk for human pilots and greater ability to operate with other systems, he said.

Budget pressures will result in a “greater emphasis on affordability, specifically reducing life-cycle cost, and providing alternatives to expensive capabilities,” he said.

The growth in UAVs is not coming at the expense of manned aircraft, Weatherington said. “Not yet,” he said. “In the future, we may seeUCAVs that can augment” or replace F-16s and F-18s for the air-to-ground role, he said, referring to unmanned combat air vehicles. “Offensive and defensive air-to-air will take more time.”

Weatherington said he anticipated more competition among suppliers for naval drones, including the Unmanned Carrier Launched Airborne Surveillance and Strike system, or Uclass, and the Medium-Range Maritime Unmanned Aerial System, or Mrmuas, and for subsystems such as data links, ground stations and payloads.

The transition to open software architecture on ground control stations “will open up competition to small businesses, and move away from the proprietary nature of earlier” systems, he said.

Michael Ciarmoli, an equity analyst with KeyBanc Capital Markets Inc. in West Conshohocken, Pennsylvania, said in a telephone interview that companies that make optics and sensors such as FLIR Systems will see “pull-through demand” from the military’s need for drones. He has a “buy” rating on FLIR in part because of the success of its “Star SAFIRE” imaging sensors.

Companies also see a growing market for stealth technology, such as Lockheed Martin Corp.’s

Pentagon's Drone Surge Includes \$5.3 Billion for General Atomics

RQ-170 Sentinel stealth drone. The CIA used radar-evading stealth drones on missions to monitor Osama bin Laden's compound in Abbottabad, Pakistan, in the months before the May 2 raid in which Navy SEALs shot and killed the al-Qaeda leader, the Washington Post reported May 17, citing unnamed U.S. officials.

"We see real utility" for drones in the reconnaissance and surveillance field with "the long-dwell, persistent capability," Robert Stevens, chief executive officer of Bethesda, Maryland-based Lockheed Martin, said in an interview.

"We are investing considerable focus on increasing levels of autonomous performance for these vehicles" that will enable drones to fly missions without a pilot on the ground directing them, he said. Advances in artificial intelligence may enable planes to fly without ground crews operating them and save costs, he said.

Stevens declined to discuss Lockheed's development of stealth drones.

AAI Corp., a unit of Textron Systems Corp., is working with its parent Textron Inc., a Providence, Rhode Island-based company whose units include Bell Helicopter, to develop new drone models that meet the Pentagon's needs for larger unmanned aerial vehicles, according to Steven Reid, vice president of unmanned aircraft systems at AAI.

"We are looking at where investments are going to be made and responding with appropriate programs," Reid said in a telephone interview. The company makes the RQ-7 Shadow used by the Army and Marine Corps at the tactical level. "While we are doing well in our particular market segment," the Pentagon's future growth in drones is more in the larger class of systems, he said.

Perhaps no company better anticipated the higher-altitude drone market than closely held General Atomics -- through its affiliate, General Atomics Aeronautical Systems Inc. of Poway, California -- whose defense business has surged in the past decade. The company received \$1.9 billion in federal contracts in fiscal 2010, up from \$111 million in fiscal 2001, according to data compiled by Bloomberg.

The Reaper, one of several unmanned platforms the company makes, will be a continuing source of revenue. The Air Force plans to spend another \$5.31 billion procuring 240 more Reapers through fiscal 2016, bringing the total inventory to 396, according to budget documents. The overall cost of the program, including research and development, is estimated at \$12.5 billion, according to Pentagon acquisition documents.

Kimberly Kasitz, a spokeswoman for General Atomics Aeronautical Systems Inc., said she could not provide comment.

Richard Aboulafia, vice president of analysis at the Teal Group, a Fairfax, Virginia-based

Pentagon's Drone Surge Includes \$5.3 Billion for General Atomics

consulting company, said in a telephone interview that UAVs are “a great talking point for future budget reduction, but a lot of these missions might just revert to more expensive manned aircraft.”

Drone costs range significantly. General Atomics’ \$28 million Reaper, for example, is a fraction of Northrop Grumman’s \$176 million Global Hawk, according to the Government Accountability Office. Bigger stealth variants may cost even more. By comparison, Boeing Co.’s F/A-18 Super Hornet costs about \$106 million.

Gunzinger of CSBA, who served as the deputy assistant secretary of defense for forces transformation and resources in the Bush administration, said the drone demand will grow as the U.S. seeks technology that can penetrate sophisticated air defense systems, such as those in China or Iran.

“The trend toward more survivable unmanned platforms is unmistakable,” he said, “and not just for strike and surveillance, but for airborne electronic attack and other missions.”

DoD Testers Slam Global Hawk

Report: DoD testers slam Global Hawk

By [Philip Ewing](#) Tuesday, June 7th, 2011 8:32 am

The latest version of the Air Force's Global Hawk unmanned surveillance jet is not ready for prime time, reports John Bennett in The Hill newspaper. Based on a DoD ODT&E report, Bennett's story doesn't make it sound like these things were falling out of the sky, but it does appear they're performing well short of what the Air Force needs.

[Wrote Bennett:](#)

The report found that the drones provided only about 40 percent of "requested intelligence, surveillance and reconnaissance (ISR) coverage when used at low operational tempos."

A subsystem fitted onto the Block 30s that is designed to gather intelligence signals, such as communications or electronic signals given off from radioactive events, "provides ... limited operational utility" at detecting, identifying and locating some radar and communications signals, the report said.

That same system — due to "technical performance deficiencies and immature training, tactics, techniques and procedures" — fails to provide "actionable" signals on intelligence, the testing shop found.

For those and other reasons, Michael Gilmore, the Pentagon's director of operational testing and evaluation, deemed the Block 30 variant "not operationally suitable."

So the newest Global Hawks have poor availability, defective sensor systems, and, perhaps most interestingly, "immature training, tactics, techniques and procedures." What could that mean — might airmen not know how to take full advantage of what their UAVs can do?

Whatever the reason, Bennett's story, with its Hill-focused audience, could force Congress to confront a reality that others in the defense game have long known about, he writes:

The Global Hawk program has battled cost increases and technical issues for years, but has avoided scorn from a large number of lawmakers.

In the study, Gilmore concluded the drone failed to give war fighters what they need from it the most: a high-flying platform that can gather ISR data for extended periods of time.

"Global Hawk long endurance flights do not routinely provide persistent ISR coverage

DoD Testers Slam Global Hawk

due to low air vehicle reliability,” the Gilmore-signed report states.

GAO: DoD Space Acquisitions Threatened by Poor Oversight

GAO: DoD space acquisitions threatened by poor oversight

June 1, 2011 — 10:33am ET | By [Molly Bernhart Walker](#)

Two acquisitions--Space Fence and the Joint Space Operations Center Mission System (JMS)--that are critical to space situational awareness will begin within 2 years, but face significant and inherent challenges due to the number of governmentwide organizations and assets involved, according to a Government Accountability Office [report](#) (.pdf).

"While the recently issued National Space Policy assigns [space situational awareness] responsibility to the Secretary of Defense, the Secretary does not necessarily have the corresponding *authority* to execute this responsibility," according to the GAO report released May 27 (emphasis original in the quote). The report is an unclassified version of a classified report issued in February 2011.

Report authors warn the House Armed Services strategic forces subcommittee that unclear management and oversight authorities could lead to the use of immature technologies and capability delivery in a single, large increment, rather than more incremental deliveries--what GAO described as a preferable method of delivery.

To safeguard against the delivery of a large, poorly developed technology, the Secretary of Defense should direct the under secretary of defense for acquisition, technology and logistics to ensure that all critical technologies for Space Fence and JMS are mature and demonstrated in a realistic or operational environment, recommended report authors. This may require JMS to be divided into separate, smaller increments, in order to ensure cost, schedule and performance goals are met, the report says.

A DoD response assured GAO that all critical technologies will be assessed as part of milestone B--or the product development and engineering/manufacturing phase. In a response, authors reiterated that GAO's "best practices work" and DoD should ensure critical technologies are identified and matured by development start.

"As currently planned, the JMS effort will not have assurance that all needed technologies will be mature when needed and that cost estimates--based on the development of all five releases--are reliable as of the start of product development," wrote report authors.

The report also recommends that if Space Fence and JMS do move forward with less

GAO: DoD Space Acquisitions Threatened by Poor Oversight

mature technologies, available backup technologies should be identified. In a response, DoD said backup technology would be most appropriately addressed after milestone B--during system integration as part of the engineering/manufacturing phase where overall system-level risks are considered, according to the report.

Again, GAO responded saying DoD's timeline would have it assessing technologies too late, rather than prior to system development.

"[Earlier] assessment could provide knowledge needed to determine whether the acquisition program is still worth pursuing or what tradeoffs would need to be made with other investments should additional resources be required," wrote report authors.

The Defense Department has made progress in improving SSA capabilities--particularly with a space-based sensor recently launched by Air Force--but it is too early to tell if this capability will effectively address SSA shortfalls, making the success of Space Fence and JMS all the more critical, says the GAO.

For more:

- see [GAO-11-545 \(.pdf\)](#)

5 Technologies That Will Shape the Web

5 Technologies That Will Shape the Web

Innovations that will make the web smarter and sleeker and irresistibly more social, too

By ELISE ACKERMAN, ERICO GUIZZO / JUNE 2011



Illustration: Carl DeTorres

This is part of *IEEE Spectrum's* special report on the battle for the future of the social Web.

It was 1997—eons ago, in Internet years—and the Web was only beginning to take off. People used dial-up modems to get online, and Netscape Navigator was the browser of choice. Google was still a research project of two Stanford students, and Facebook...well, Mark Zuckerberg was a 13-year-old having his Star Wars-themed bar mitzvah.

5 Technologies That Will Shape the Web

21

*Sergey Brin
& Larry Page*

10

*Mark
Zuckerberg*

1

Justin Bieber

**AGE IN
1994,
WHEN
THE FIRST
VERSION
OF THE
NETSCAPE
BROWSER
CAME OUT**

Flash forward to 2011. The Web has since reinvented itself time and again: when businesses embraced it in the late 1990s, when [Google](#) dominated search in the early 2000s, when [user-generated content](#) became prominent in the mid-2000s. Today the Web is going through another reinvention, morphing into a place where our social interactions are ever more important. And the main force behind this phenomenon is, of course, [Facebook](#), led by Zuckerberg, now a 27-year-old billionaire.

So where will the Web go next? We asked two dozen analysts, engineers, and executives to describe what technologies they think will shape our online experiences in the next several years. Their predictions could easily fill this entire issue, but we distilled their wisdom into a more palatable list of five key technologies that our sources mentioned most frequently.

We also asked six of the experts to tell us what these technologies mean for today's dueling titans, Google and Facebook. What challenges do they face? Who's got an advantage? You'll find their comments sprinkled throughout these pages.

5 Technologies That Will Shape the Web

Lists like this are nothing if not contentious. Some critics will say we overlooked more crucial trends. Others will claim our technologies are already history. So we want to know what you think. Join the discussion in the comment section below.

1. The Mobile Web Will Be a Smarter Web



In a watershed moment in the history of computing, global shipments of smartphones exceeded those of PCs for the first time in the fourth quarter of 2010. The rise of mobile devices is indeed staggering in its pace and scale. Every day, carriers activate 350 000 phones running Google's Android operating system. An estimated 15 percent of Google's search volume now comes from mobile devices. More than 10 billion apps have been downloaded from Apple's App Store.



When we talk about mobile as a disruptive technology, we need to talk about social. Google is winning the Web, but Facebook is winning social. I see Google really flailing around social. They are trying to figure it out, but they are coming late to the game.
—*Gina Trapani, Developer, ThinkUp, smarterware.org*

Today a fierce battle is under way between Google's Android and Apple's iPhone. But let's put that aside and focus on how mobile technology is transforming the user experience. For many people mobile devices are becoming the favored portal to their online social lives. We're using our phones to voice opinions, publish photos, play games, and check on friends. More than 250 million users access Facebook on their mobile devices, and 40 percent of all tweets come from mobile platforms. Already the iPhone 4 is poised to become the most popular camera among Flickr users. Experts say this is just for starters. The powerful blend of mobile and social capabilities

5 Technologies That Will Shape the Web

will inspire new products and services and become the foundation for new ways to work, shop, and entertain ourselves. The key element propelling this transformation? Context.



Mobile phones mean that people want information in context. So Google's challenge is to give people personalized recommendations on the fly, which is different from a list of search results. Facebook is well placed in this regard, because they have the social context for search on mobile phones.

—**Richard MacManus**, Blogger, *ReadWriteWeb*,
readwriteweb.com

Most of the time when you use your phone, you're immersed in a specific context: There's the location, the day and time, what you're doing there, what is nearby, whether you've been there before. There's also your social graph—the connections among individuals, as well as among individuals and objects—with bits of data that are relevant to that context (whether, say, any friends have shared information about that location). The future of mobile computing will be all about how big companies and start-ups alike develop technologies—data analytics and machine learning algorithms, for example—capable of making sense of context data to provide better search results, advertising, and other services.

To see where this is going, consider one piece of context information that companies are already exploring: geolocation. Facebook launched a service called Places, and Google has Latitude; location start-ups include Foursquare and Gowalla. Using GPS and Wi-Fi data from people's phones, these services offer location-specific information and deals. If you're at a store, you might receive a discount coupon; if you're at a bar, you'll see what friends have said about the place and whether any of them are nearby. So what our mobile devices are doing is linking the digital world to the real world—and as a result, new applications will become possible and people will become ever more connected to other people.

"You're going to see the same kind of changes to industry and business that you saw when the Web became popular," says Dennis Woodside, a Google vice president, "but it's going to happen much faster."

2. Video Is Poised to Inundate the Web

5 Technologies That Will Shape the Web



Answer quickly: What's the world's second-largest search engine? If you said Yahoo or Bing, you'd be wrong. The answer is YouTube.

Each month, YouTube users all over the world collectively spend some 2.9 billion hours—that's 331 050 years, if you're wondering—on the site. More video is uploaded to YouTube in 60 days than the three major U.S. networks created in 60 years.



We have an increasing expectation that we should be able to watch movies and entertainment whenever we want to. Why do I have to watch "American Idol" at night on a certain channel? Why can't I just pull it up on my iPad and watch it when I want to watch it?

—**Robert Scoble**, *Blogger*, [Scobleizer](http://Scobleizer.com), scobleizer.com

Analysts say that YouTube, acquired by Google in 2006, is just the beginning trickle of a video flood that will swamp the Web. Indeed, video traffic has already surpassed peer-to-peer as the dominant form of data flowing in telecommunications pipes. Movies streamed by [Netflix](http://Netflix.com) alone can make up as much as 20 percent of U.S. broadband traffic on any given night. As more TV programming shifts to the Web, TV sets themselves are becoming Net-enabled devices optimized for video consumption. Smartphones that make it easier to produce, watch, and share video only help to accelerate this trend.

But the future of Web video is not only that there will be more of it—how we watch it is also changing. That's because the Web is enhancing the social nature of video. We love to talk about what we watch—some people now tweet in front of the TV during shows and sports—and we love to recommend things to one another.

5 Technologies That Will Shape the Web



Google has more to be worried about with video than Facebook does in the sense it has more to lose. YouTube is a hugely popular video-sharing site, but it faces some threats. For example, it needs to make the transition to professional content, and that transition has been hard.

—**Danny Sullivan**, *Blogger, Search Engine Land, searchengineland.com*

And here's where the social Web comes in. The social graph could be the basis of a powerful recommendation engine. Indeed, Facebook recently teamed up with Warner Bros. to offer streaming movies for rent, starting with The Dark Knight in March. Facebook's move into distribution is a big threat to cable companies' pay-per-view services; to YouTube, which has long sought more professional content; and even more so to Netflix, now the dominant force in online movie rentals. Facebook's advantage is its massive user base and the fact that it can use people's social connections, their comments, and "likes" to suggest movies in a very effective way. Because online video's attractiveness to users makes its revenue potential gigantic, companies are reorganizing their software and network infrastructures to accommodate it. That focus has touched off a major battle over standards. More and more Web video is relying on a patent-encumbered encoding technology known as H.264. Google, which says it favors an open, free-for-all video format, has dropped support for H.264 and is pushing instead for an alternative called WebM. A resolution should emerge when a new Web standard, HTML5, becomes official. HTML5 will specify which video formats—contenders include H.264, WebM, and others—all browsers should support. David Recordon, senior open programs manager at Facebook, says that no matter which format prevails, it will lead to richer applications both on the Web and on mobile devices, making it easier for ever more people to create and consume video.

3. Everyday Objects Will Join Our Social Networks

5 Technologies That Will Shape the Web



After the emergency at Japan's Fukushima Dai-ichi nuclear plant early this year, government agencies and individuals set up Geiger counters to measure radiation. Like many sensors today, these Geiger counters post their measurements to the Web, which lets people pool the data and crowdsource the monitoring of radiation levels. Welcome to the Internet of Things, where data from scientific instruments, embedded sensors, and a vast assortment of Net-connected objects will eventually eclipse information produced by humans.



Many of these connected devices will use Android, so Google will benefit from the trend, though it has to figure out how to integrate their data in their search index. Facebook isn't there yet, because what is missing is the social layer in those devices. But Facebook is so big—they will figure something out.

—**Jeff Clavier**, Investor, SoftTech VC, softtechvc.com

Actually, it's already happening. Carnegie Mellon University researchers are developing sensors to monitor buildings, roads, and bridges. A high-tech pedometer made by Fitbit monitors your movements and lets you share your exercise habits with your friends. Last year, toy maker Mattel unveiled an electronic tag that sends a tweet whenever a dog moves or barks.

First proposed more than a decade ago, the Internet of Things is finally taking shape, thanks to ever cheaper electronics, improvements in wireless technologies, and the availability of DIY electronics like the Arduino, a popular open-source microcontroller. Mapping data from ubiquitous sensors to our social graphs will provide valuable information about ourselves and our surroundings. People will find ways to use these streams of information to their advantage, in ways that we can't necessarily anticipate now but that will surely test our boundaries for privacy and publicness. Don't be surprised when your fridge joins Facebook.

5 Technologies That Will Shape the Web



Sensors will pump a ton of new data into the Internet. What's most fascinating is what will be built on top of that new data, which makes it likely to produce deeply disruptive new start-ups and companies. The next Google or Facebook may well be an Internet of Things company.

—**Richard MacManus**, Blogger, *ReadWriteWeb*, readwriteweb.com

4. Web Data Will Explode, and That's a Good Thing



If the early days of the Web ignited an explosion of data, what we're seeing today is more like an A-bomb blast. Google executive Marissa Mayer has said that data are proliferating at a rate that outpaces Moore's Law. According to research firm IDC, the amount of data created globally last year surpassed 1 zettabyte—enough to fill a billion 1-terabyte hard drives.

This unprecedented data accumulation has led to a tech arms race of sorts, with companies seeking new ways of storing, managing, and analyzing information. The industry has dubbed this trend "big data."

Google, of course, was a pioneer in the development of data-crunching technologies. It created tools such as MapReduce, a set of superefficient algorithms for distributing and processing large blocks of data, and built supersecret data centers that work like "warehouse-sized computers," as some Google researchers have described them.



Facebook is trying to be hegemonic when it comes to your profile. Facebook Connect is brilliant because of that. They couldn't be the one place where everyone went on the Web, but they could be the profile that everyone links to.

Charlene Li, Analyst, *Altimeter Group*, altimetergroup.com

5 Technologies That Will Shape the Web

This computing capability is at the heart of what makes Google's search offerings so powerful. It also lets the company discover insights about what people are collectively thinking, the seasonality of the flu, and the popularity of words. Peter Norvig, Google's director of research, says that having more data opens the door to new kinds of theories and models—new ways of thinking about the world.

But today's big data will be different from tomorrow's. A large fraction of today's data consists of Web pages that companies like Google can crawl, process, and present to users when needed. In the future, however, users will consume and produce ever more data in near real time.



Google has so much data that they have been sucking up from the Web for so long, but Facebook has structured data that is people-centric. That is really powerful, especially with mobile happening and people wanting to find other people, versus Web pages. Facebook's big data is a lot more interesting than Google's.

—*Gina Trapani, Developer, ThinkUp, smarterware.org*

The new data will come in great part from the social Web. Already, Facebook users share more than 30 billion pieces of content—Web links, news stories, blog posts, photos—each month. Twitter users generate more than 155 million tweets per day (up from 55 million one year ago). What's more, both companies are establishing themselves as platforms for data aggregation, granting other companies access to the results through APIs, or application programming interfaces. (Facebook Connect, which allows sites to access public data from Facebook users, is one such API.) The growth of these interconnections, of course, spawns still more online data, in a widening spiral.

It's a spiral that is leaving Google, perhaps more than anyone else, dizzy: Real-time and social search poses the greatest threat to the company's search hegemony. As Facebook, Twitter, and other social-oriented sites amass vast volumes of data and connect this data to people's social graphs, they might be able to help users find information in ways that Google can't.

As this battle unfolds, tech companies, including innovative start-ups like Cloudera,

5 Technologies That Will Shape the Web

race to build better big-data technologies: radically new server architectures, database systems very different from classic relational schemes, novel language frameworks that combine the best aspects of various programming languages. They're also mobilizing highly specialized teams of "data scientists." Interestingly, although the companies are secretive about their tech arsenals, they rely a great deal on open-source code, sometimes even collaborating on open-source projects that all can use. Experts say that innovations in big data will lead not only to better online experiences but also to new data-driven services and even scientific discoveries.

5. Voice and Gestures Will Change Human-Computer Interaction



In the past 30 years, processors have steadily gotten faster, storage systems have mushroomed in capacity, and even monitors have lost weight and gained higher resolutions. But the way we interact with computers—with a keyboard and mouse—hasn't changed a whit.

Now human-computer interaction is really evolving. Smartphones and tablets have popularized touch screens, doing away with physical keyboards and creating an interface that even toddlers can intuitively operate. Next is voice. Google has already voice-enabled its search app for Android: Speak and the program will search. Another app will translate sentences between Spanish and English in near real time.



Some disruptions are difficult because they require large investments. Natural interfaces are really hard; they require a huge amount of R&D. What is great about Kinect is it removes a layer of technology between me and the content.

—**Charlene Li**, Analyst, Altimeter Group, altimetergroup.com

5 Technologies That Will Shape the Web



If you look at Google, they have tons of people who are working on voice. It is something that is almost required for Android. But I don't think that the new interfaces are causing much disruption in terms of the incumbents. This is where we see evolution; we don't see revolution.

—**Jeff Clavier**, Investor, SoftTech VC, softtechvc.com

But the next wave of interfaces will involve...waving. Last year, Microsoft launched Kinect, a 3-D motion sensor for its Xbox 360 game console. The device projects a pattern of infrared dots, invisible to the naked eye, on the environment. Then it uses a sensor to "see" the dots, deriving their distance based on how objects and people deform the pattern. Some speculate that Microsoft may integrate Kinect controls into Windows. (Cue Tom Cruise waving frenetically as he operates a futuristic computer in *Minority Report*.)

Experts say the latest innovations in natural interfaces provide a glimpse of a fast-approaching future in which people will interact with the Web very differently—not only by typing and touching but also by talking and gesticulating before our devices.

"We want to make technology disappear," says Alex Kipman, Kinect's project leader at Microsoft.

Helping Chips Sip Power

Helping Chips to Sip Power

Silicon Valley Start-Up Offers Technique to Cut 'Leakage,' Extend Battery Life

By [DON CLARK](#)

A team of Silicon Valley veterans is claiming they can reduce power consumption in computer chips by 50%, potentially extending the battery life of portable devices and helping chip manufacturers keep pace with giants like [Intel Corp.](#)

Their start-up, SuVolta Inc., on Monday plans to announce that the semiconductor arm of Japan's [Fujitsu Ltd.](#) is licensing its technology to make chips starting next year. Assuming other companies follow suit— some analysts say the closely held company could have a broad impact on the industry.

"The technology could have a very, very significant position," said Handel Jones, president of International Business Strategies, a consulting firm specializing on the chip market.

The topic of power consumption has swelled in importance with the increased use of cellphones and other portable devices, all of which have power-hungry chips. Building more energy-efficient chips becomes harder as manufacturers shrink semiconductor circuitry to the point that electrical current tends to leak from microscopic components.

Intel, a leader in miniaturization, in May said it would shift to a new three-dimensional structure in its transistors to boost performance while controlling power consumption. SuVolta believes it can help other chip makers achieve similar power savings without such a radical change in manufacturing.

The company, which has previously kept mum about its plans, was founded in 2005 as DSM Solutions Inc. and later modified its name and management

Helping Chips Sip Power

team. Key recruits include Scott Thompson, a former University of Florida professor who helped develop chip production processes during 12 years at Intel and became SuVolta's chief technology officer.

He focused efforts on a key contributor to power leakage—variations among individual transistors in the voltage needed to switch them on or off. Such variations have become more common as transistors gets smaller, he said, making it more difficult to control the addition of materials known as dopants when creating channels that conduct electricity.

Mr. Thompson said he came up with a set of techniques to create transistors that minimize such voltage variations, while requiring few changes to current manufacturing practices. He isn't disclosing many details yet, but said the techniques cut current leakage by 50% and allow chips that now typically require at least 1 volt to operate with 0.7 volt—with 0.5 volt a target for the future.

"It is compatible with all the things that people have been doing," said Bill Joy, a partner at SuVolta investor Kleiner Perkins Caufield & Byers, who is better known as co-founder of Sun Microsystems. Chip manufacturers "don't have to spend a decade figuring out how to take the next step," he said.

Proving SuVolta's claims will take time. The company says it has built working chips with Fujitsu using a mature manufacturing process. But moving to advanced production processes that create smaller circuitry will be crucial to play a role in chips for high-volume devices like cellphones, Mr. Jones said.

Besides Mr. Thompson, SuVolta's technical team includes Pushkar Ranade and Lucian Shifren—who also worked at Intel on production processes—and Nick Kepler, former vice president of products at chip manufacturer Globalfoundries.

SuVolta says the first investor in its earlier incarnation was Andreas

Helping Chips Sip Power

Bechtolsheim, another Sun co-founder who was also [Google](#) Inc.'s first outside investor. Its chief executive is Bruce McWilliams, former CEO of a Silicon Valley company called [Tessera](#) Inc. that also licenses technologies to chip makers rather than sells products.

Mr. McWilliams isn't disclosing how much SuVolta tends to charge, but says he plans to emulate other licensing companies known for reasonable royalties. "I like to think of our company as the Dolby of Silicon Valley," he said.

First Graphene Integrated Circuit

First Graphene Integrated Circuit

IBM researchers take next step in building graphene-based electronics

By NEIL SAVAGE / JUNE 2011

9 June 2011—IBM researchers have built the first integrated circuit (IC) based on a [graphene transistor](#)—another step toward overcoming the limits of silicon and a potential path to flexible electronics.

The circuit, built on a wafer of [silicon carbide](#), consists of field-effect transistors (FETs) made of [graphene](#), a highly conductive chicken-wire-like arrangement of carbon that's a single atomic layer thick. The IC also includes metallic structures, such as on-chip inductors and the transistors' sources and drains. The work is described in this week's issue of *Science*. Researchers say that graphene, which has the potential to make transistors that operate at terahertz speeds, could one day supplant silicon as the basis for computer chips.

Several groups have built transistors out of graphene; the IBM team, led by [Phaedon Avouris](#) at the Thomas J. Watson Research Center, demonstrated one last year that operated at 100 gigahertz—more than twice as fast as a silicon transistor of comparable dimensions. But as Keith Jenkins, one of the scientists involved in the new research, points out, "a transistor by itself is no good unless you connect it to something."

The circuit the team built is a broadband radio-frequency mixer, a fundamental component of radios that processes signals by finding the difference between two high-frequency wavelengths. "It's a completely ubiquitous circuit," Jenkins says. The device, which is a proof-of-concept and not designed to be an optimal commercial component, handles frequencies up to 10 GHz. "Ultimately, we should be able to go a lot faster," Jenkins says. "This is not a limit at all."

The tricky part was integrating the [graphene FET](#) with other components—"a pretty difficult engineering challenge" that took about a year, Jenkins says. There are two main difficulties: One is that the metals used to make other parts of the circuit—aluminum, gold, and palladium in this instance—don't adhere very well to the graphene. The other is the fact that graphene, being only a single atom thick, is easily

First Graphene Integrated Circuit

damaged by standard semiconductor etching processes. One way the team addressed the damage problem was to grow the graphene on a silicon-carbide wafer, then coat it with a common polymer, PMMA, and a resist that was sensitive to jets of electrons used in electron beam lithography. That allowed them to protect the graphene they needed during processing but also remove it where it wasn't wanted.

One remarkable feature is that the performance of the device didn't change very much when its temperature went from 300 to 400 kelvins (about 27 °C to 127 °C). That means a graphene circuit won't have to be overdesigned to compensate for temperature changes, potentially leading to a less-complex and less-expensive circuit.

Tomás Palacios, an electrical engineer at MIT, called the device "a nice piece of work," adding, "Although there is still a lot of work to be done to improve the device and circuit performance, it represents an important step forward to useful circuits."

The IBM team identified a couple of steps that could improve the performance, such as using a thinner dielectric layer in the transistors. Jenkins says the team is also looking for better materials for the contacts, because anything that touches the graphene has the potential to degrade its electron mobility. The next component he'd like to build is a graphene-based amplifier, though the electronic properties of the material make that challenging.

It will be several years before graphene devices are ready to displace conventional silicon circuits, which are expected to start hitting their limits later this decade. But Jenkins says progress has been remarkably fast with graphene, which was isolated only in 2004. Beyond surpassing the performance of silicon, the material, which is strong, transparent, and bendable, could lead to flexible printed electronics. Applications could include cellphones stitched into clothing or GPS receivers on soldiers' uniforms. Says Palacios: "I think that the exciting opportunity of graphene is to be able to integrate these devices/circuits into arbitrary substrates, from plastics to silicon and glass. This integration will allow us to have graphene-based electronics everywhere. It is what I call 'ubiquitous electronics.' "

About the Author

First Graphene Integrated Circuit

Neil Savage writes about strange semiconductors and amazing optoelectronics from Lowell, Mass. In May 2011, he wrote about a single-laser system that transmits a record 26 terabits per second of data.