



CyberPro

Volume 3, Edition 2
January 28, 2010

Keeping Cyberspace Professionals Informed

<p style="text-align: center;">Officers</p> <p>President Larry K. McKee, Jr.</p> <p>Chief Operations Officer Jim Ed Crouch</p> <p>----- CyberPro Editor-in-Chief Lindsay Trimble</p> <p>CyberPro Research Analyst Kathryn Stephens</p> <p>CyberPro Archive</p>	<p>The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest and to keep subscribers who are involved in the development of Cyber-related concepts and initiatives informed on items of common interest. The newsletter and the information contained therein are not intended to provide a competitive advantage for any commercial firm. Any misuse or unauthorized use of the newsletter and its contents will result in removal from the distribution list and/or possible administrative, civil, and/or criminal action.</p> <p>The views, opinions, and/or findings and recommendations contained in this summary are those of the authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or National Security Cyberspace Institute.</p>
<p style="text-align: center;">To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.</p> <p>Please contact Lindsay Trimble regarding CyberPro subscription, sponsorship, and/or advertisement.</p>	

All rights reserved. CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.



TABLE OF CONTENTS

This Week in CyberPro	6
Education & Training	7
Cyberspace – Big Picture	8
Merging disparate networks brings new complexity for IT security and risk management staff	8
Internet heading for ‘perfect storm’	8
Internet scams go after those hit hardest by recession	8
Lockheed enters next phase of National Cyber Range project	9
Cyberspace – U.S. Government	9
Clinton demands unrestricted ‘Net access’	9
Is Hillary Clinton launching a cyber cold war?	10
Google poses Obama a problem.....	10
80% of government Web sites miss DNS security deadline	10
Senate to hold cybersecurity hearing	11
NIST releases update to smart grid standards	11
FBI Director to chronicle the evolution of cyber threats at RSA Conference 2010	11
Is Boeing’s new 747 hackable?	11
FCC looks at ways to assert authority over Web access	12
U.S. Cyber Czar Announced	13
The cybersecurity czar’s first big test	13
Obama’s cybersecurity czar to speak at DoD’s Cyber Crime Conference	13
Cyberspace – Department of Defense (DoD)	14
Integrated cyber operations	14
Cyber situational awareness.....	14
Senior General says U.S. needs to move faster on cyber defense.....	14
Air Force issues second call for network attack capabilities	14
Back away from GPS: AF Chief.....	15
Air Force awards cybersecurity deal.....	15
Cyber is the focus	15
Army mulls realignment to fortify cyber command.....	15
Navy cyber forces established.....	16
Poisoned PDF pill used to attack U.S. military contractors	16



'Cyber Genome Project' kicked off by DARPA	17
U.S. faces critical lack of (mad) computer scientists	17
DARPA: U.S. geek shortage is national security risk	17
Interview with Mark Orndorff of DISA, part I	17
Interview with Mark Orndorff of DISA, part II	18
Cyberspace – International	19
Iran accuses U.S. of using Internet against it	19
More cyberattacks likely from group that took down Chinese search engine	19
Why the 'China virus' hack at U.S. energy companies is worrisome	19
Information warfare: South Korea is at war	19
South Korea sets up cyberwarfare unit to repel NORK hackers	20
Gates looks to India for cyber cooperation	20
Information warfare and Indian national security	20
China hackers tried to hit India, <i>Times</i> says	20
Chinese hackers target PMO	21
Australia recruits cybersecurity experts	21
Cyber warfare HQ opens its doors	21
UK warfare debate	21
UK.gov dismisses Tory claims UK cyberspace is defenseless	22
French Government calls on Internet users to abandon Internet Explorer	22
Multinational cyber defense agency to expand membership	22
Russian hackers jam automobile traffic with porn	22
Google vs. China	23
Hacking risks persist even if firms leave China	23
China's cyberwar goes beyond Google	23
Google: Doing the right thing	23
China won't yield to Google on censorship, analysts say	23
Security experts dissect Google China attack	24
Microsoft's Ballmer: We're staying in China	24
China defends censorship after Google attack	24
A new era of Internet control	24
McAfee: China attacks a 'watershed moment'	25
China: We are biggest victim of hacking	25
Security researcher IDs China link in Google hack	26



CyberPro

Volume 3, Edition 2
January 28, 2010

Keeping Cyberspace Professionals Informed

Google suspects Honker Union to be the culprit of its recent cyber attack	26
What's really at stake in Google vs. China	26
Google didn't kowtow and neither should you	26
China attacks Clinton's Internet speech as 'harmful' to relations	27
China rejects accusations on Google hack, Internet freedom	27
China steps up defense of Internet controls	27
Google may keep some Chinese operations.....	28
Cyberspace Research	28
Declining confidence in social networking security.....	28
Mal-Bredo A virus spreads via social media.....	29
Report: DDoS attacks still growing, but at slower rate	29
Cyberspace Hacks and Attacks	29
Fearing hackers who leave no trace.....	29
Juniper, Symantec investigating after Google attack	30
Yahoo reportedly hit by China hackers.....	30
Hackers used rigged PDFs to hit Google – and Adobe, says researcher.....	30
Verisign mistaken about Adobe flaw's part in Google attack	30
DIY cybercrime kits power growth in Net phishing attacks.....	31
IE attack code out in the open	31
Whirlpool's Kitchenaid.com remains malware infected for 5 months	32
iPhone hacker says he's also cracked PlayStation 3	32
Unknown computer virus hits University of Exeter network in UK.....	32
Hundreds of Network Solutions sites hacked	32
Microsoft perform DOS on Perl Testers	33
Cyberspace Tactics and Defense	33
Gmail ups security after Chinese attack	33
SAIC to acquire CloudShield	33
Lockheed Martin invests in cyber security talent and workforce development	34
JavaScript hack enables flash on iPhone.....	34
How not to deploy SSL	34
Thales, Voltage Security to deliver End-to-End Encryption, key management solutions.....	35
Hackers are defeating tough authentication, Gartner warns	35

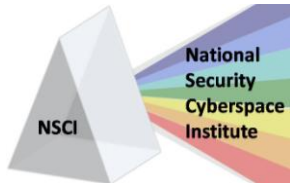


CyberPro

Volume 3, Edition 2
January 28, 2010

Keeping Cyberspace Professionals Informed

Cyberspace - Legal	35
Google-China row spurs on cyber bill.....	35
McKinnon wins review of extradition for hacking.....	35
Law firm in Green Dam suit targeted with cyberattack.....	36
Nebraskan pleads guilty to 2008 Web attack on Scientologists.....	36
Cyberspace-Related Conferences.....	37
Cyberspace-Related Training Courses	39
Cyber Business Development Opportunities	41
Employment Opportunities with NSCI.....	44
CyberPro Content/Distribution	44



THIS WEEK IN CYBERPRO

BY LINDSAY TRIMBLE, NATIONAL SECURITY CYBERSPACE INSTITUTE, INC.

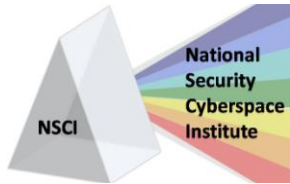
If you've been plugged into the news at all this month, you've seen the headlines regarding Google vs. China. Immediately following the discovery that recent cyber attacks originated in China, Google threatened to pull all operations out of the Asian nation. Since then, Google is in talks with the Chinese government to keep some operations in China ([page 28](#)). Google executives reportedly want to maintain their access to China's engineering talent, growing online advertising and mobile phone markets. An article in *Forbes* praises Google's decision to pull operations out, calling it a "moment of moral clarity" ([page 23](#)). Some analysts have questioned whether the decision to withdraw is fully due to ethical concerns regarding censorship ([page 23](#)). Others are saying that how the Obama administration chooses to react to the cyber attacks will be Howard Schmidt's first test as the new U.S. cybersecurity czar ([page 13](#)). U.S. Secretary of State Hillary Clinton has called on the Chinese government to provide an explanation of the attacks and said she plans "to make unrestricted access to the Internet a top foreign-policy priority" ([page 9](#)).

Chinese authorities are defending their right to online censorship, saying that the Chinese government only censors information to guarantee state security and the secure flow of information ([page 24](#)). Chinese Foreign Ministry spokesman Ma Zhaoxu said that Chinese companies were often hit by cyber attacks and that China itself was the biggest victim of hackers ([page 25](#)). In an interview with *CNN*, Fareed Zakaria, author and host of "Fareed Zakaria: GPS," says China is having a difficult time balancing its drive for modernity and attempting to control information ([page 26](#)).

Since the attack, Google has announced that Gmail will now be encrypted by default as a guard against hackers ([page 33](#)). And on Capitol Hill, Sen. Jay Rockefeller (D-W.Va.) is pushing even harder to get his cybersecurity bill approved as soon as possible ([page 35](#)).

The military is also working to improve their cyber situational awareness. *Defense Tech's* Kevin Coleman writes that the U.S. military is the most computerized and modern force in the world, making the challenge of cyber situational awareness greater and more important than for any other military in the world ([page 14](#)). As the Air Force's 24th Air Force grows into its role as the new operational command responsible for cyberspace ([page 15](#)), the U.S. Army may also be planning a unified cyber component – the Army Cyber Command – that will include elements of communications and intelligence and will report directly to the U.S. Cyber Command ([page 15](#)). The U.S. Navy has recently established the Navy Cyber Force in Norfolk, Va., under the command of Vice Admiral H. Denby Starling II ([page 16](#)).

We hope you enjoy this edition of *CyberPro*!



EDUCATION & TRAINING



Security and Windows 7 Free Web Seminar

Built on the foundation of Windows Server 2008 and Windows Vista, Windows 7 is the desktop operating system IT professionals need to enhance their organization's desktop environment. Windows 7 provides greater security and manageability for remote and local PCs, and improves the fundamentals of performance and reliability.

Join us for this free on-demand Web seminar to learn the key security components of Windows 7 and where they can be configured and used.

Security features covered during this webinar include:

1. System and Security
2. User Access Control (UAC)
3. Windows Defender
4. Firewall Basic and Advanced
5. Network Access Protection (NAP)
6. Audit Policies
7. AppLocker
8. BitLocker - Hard Drive and To Go Encryption
9. Group Policy Objects (GPO)

[Register Now](#)



CYBERSPACE – BIG PICTURE

Merging disparate networks brings new complexity for IT security and risk management staff

SECURITY PARK
01/25/2010

Many businesses are looking for mergers or acquisitions to improve their financial position in a down market, but combining two completely different IT infrastructures and IT management processes can be difficult and complex. Each network is made up of different equipment, managed through different interfaces and governed by different policies and standards. IT departments must plan and implement network changes and determine how to consolidate devices and people in order to ensure consistent availability, security and compliance. This article discusses how organizations can use the approach of risk modeling in post-merger risk analysis. Risk modeling can help organizations quickly identify immediate risks; quantify those risks; prioritize security and compliance gaps; and focus resources on the most immediate risks. Risk modeling tools allow IT departments to understand the converged network, spot vulnerabilities, prioritize risks and manage a secure and compliant network.

http://www.securitypark.co.uk/security_article_264216.html

Internet heading for 'perfect storm'

BY: JOHN E. DUNN, TECHWORLD
01/19/2010

Arbor Networks recently released their latest annual Infrastructure Security Report survey of 132 large IP operators from around the world, and found that many service providers are worried that attacks on the cloud could cause

major global outages. The article explains that a single vulnerability in any part of the several software elements on which a cloud provider bases its services could compromise the entire virtualized cloud service and all of its customers. Respondents also named ID and credential theft, DNS cache poisoning, system compromise, Internet worms, botnets and distributed denial-of-service attacks as their other top worries. Arbor says the number of significant worries is a "perfect storm of problems" and when "considered together, they represent the greatest and potentially most disruptive set of circumstances in the history of the Internet."

<http://news.techworld.com/security/3210547/internet-heading-for-perfect-storm/>

Internet scams go after those hit hardest by recession

BY: KEVIN MCCOY, NEWSFACTOR.COM
01/13/2010

Hundreds of thousands of Americans filed complaints with the Better Business Bureau last year after falling for scams from bogus government grant offers, mortgage-foreclosure aid scams and phony job offers. The Better Business Bureau warns that most of the scams they receive attempt to take advantage of the unemployed and others struggling with the recession. The top 10 scams include ads that feature free trial offers for products such as anti-aging pills or other health products, and fake mailings that appeared to be winner notifications, which required the recipient to wire hundreds of dollars in fees or taxes.

http://www.newsfactor.com/story.xhtml?story_id=71008

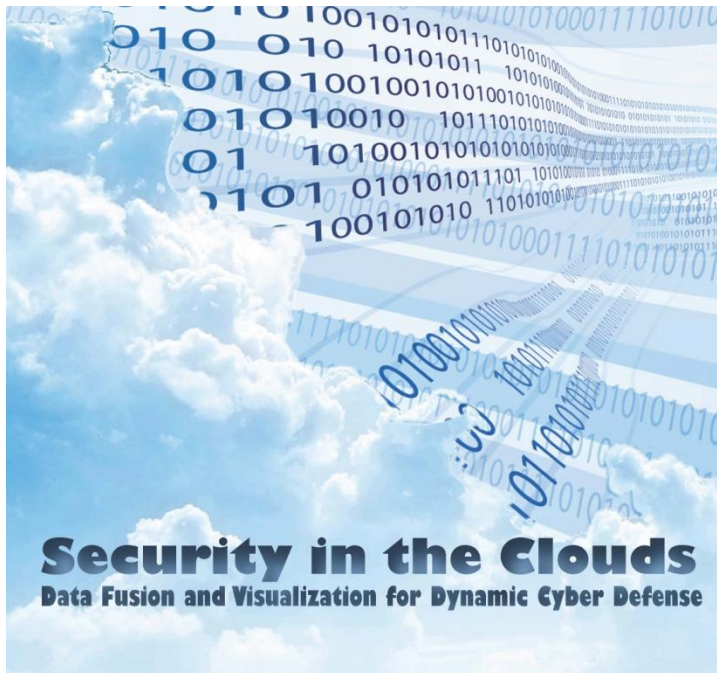


Lockheed enters next phase of National Cyber Range project

BY: DAVID HUBLER, WASHINGTON TECHNOLOGY
01/13/2010

Lockheed Martin Corp. will begin implementing Phase II of development of the National Cyber Range by building on the preliminary design created in Phase I. Phase II will culminate in the

completion of a working prototype that demonstrates the capabilities of the NCR. NCR is expected to revolutionize the nation's ability to conduct cyber operations. The estimated completion date for this phase is April 14, 2011. <http://washingtontechnology.com/articles/2010/01/13/lockheed-national-cyber-range.aspx>



- Understand common data fusion and information visualization needs across agencies
- Build on the lessons learned by other government cyber operations centers and agencies
- Foster ongoing dialogue among the cyber operations centers of the federal government

February 11, 2010
Alexandria, VA
www.afei.org

CYBERSPACE – U.S. GOVERNMENT

Clinton demands unrestricted 'Net access

FOX NEWS
01/21/2010

Hillary Clinton recently spoke about China and other nations that restrict Internet access to their citizens, saying there has been “a spike in threats to the free flow of information” and that she “plans to make unrestricted access to the Internet a top foreign-policy priority.”

Clinton also called on the Chinese government to conduct a full review following accusations

from Google that Chinese hackers had penetrated the company's computer networks. One new State Department initiative will provide financial support to “grass-roots movements” that help to promote Internet freedom and the advancement of U.S. diplomatic goals. Clinton said Internet freedom is critical to America's promotion of democracy abroad.

<http://www.foxnews.com/scitech/2010/01/21/clinton-address-internet-freedom-security/>



Is Hillary Clinton launching a cyber cold war?

BY: EVGENY MOROZOV, FOREIGNPOLICY.COM
01/21/2010

In this article, Evgeny Morozov discusses Hillary Clinton's recent speech on Internet freedom. Morozov writes that he was "taken aback" by how much "Cold War rhetoric" Clinton used. Morozov also says Clinton was too soft on China by saying they could censor whatever they like because they have different views than the United States. Clinton added that we must go after those who initiate cyber attacks, which Morozov calls puzzling because of the campaigns launched by American hacktivists. Morozov says this demonstrates the lack of a coherent view on the ethics of cyberwarfare. Morozov also says the State Department does not have a coherent view on online anonymity because they want to crack down on intellectual theft and terrorism, while protecting the rights of Iranians and the Chinese.

http://neteffect.foreignpolicy.com/posts/2010/01/21/cyber_cold_war

Google poses Obama a problem

THE SPECTATOR
01/14/2010

This article discusses the challenge that Google has given the Obama administration by threatening to shut down its operations in China because of continuous cyber attacks from Chinese hackers. Google has publicly acknowledged the attacks, "which the U.S. intelligence community has known about for almost a decade." This article even claims that U.S. intelligence has set up the largest counterintelligence effort in American history, called Byzantine Foothold and Byzantine Hades, to try to combat the attacks, although so far without success. Now that Google has decided to go public, the Obama administration must decide: "take on the Beijing regime and stand

with its own Fortune 100 companies, all of whom are victims of Chinese espionage, or ignore the problem and pretend it isn't happening."

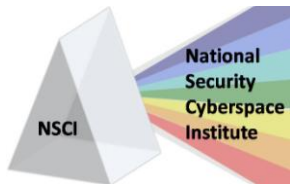
<http://www.spectator.co.uk/coffeehouse/5706898/google-poses-obama-a-problem.shtml>

80% of government Web sites miss DNS security deadline

BY: CAROLYN DUFFY MARSAN, NETWORK WORLD
01/21/2010

Mark Beckett, vice president of marketing for Secure64, says that only 20 percent of federal agencies had deployed DNS Security Extensions (DNSSEC) by the Dec. 31, 2009 deadline. DNSSEC is an Internet standard that can prevent spoofing attacks by allowing Web sites to verify their domain names and IP addresses using digital signatures and public-key encryption. Steve Crocker, CEO of Shinkuro, an R&D company engaged in DNSSEC-related work, says the OMB deadline was too aggressive and that it is a positive sign that even 20 percent of agencies were able to deploy DNSSEC. Once fully deployed, DNSSEC will have a broad impact by making it extremely difficult to forge a DNS response, ensuring that citizens who visit a federal Web site are not redirected elsewhere. Many other countries have already deployed DNSSEC on their country code domains, including Sweden, Puerto Rico, Bulgaria and Brazil. Some industry observers say the Obama administration's failure to meet the DNSSEC deadline is the result of not focusing enough on cybersecurity. Some claim there is a "lack of leadership throughout the government on cybersecurity," although OMB says cybersecurity is a top priority for President Barack Obama and that agencies are "aggressively adopting new tools and technology to ensure the safety of government information."

<http://www.networkworld.com/news/2010/01/2010-dns-security-deadline-missed.html>



Senate to hold cybersecurity hearing

BY: KIM HART, THE HILL
01/21/2010

The Senate Judiciary Committee has announced it will hold a hearing Feb. 10 on "Combating Cyber Crime and Identity Theft in the Digital Age." Witnesses include Ari Schwartz of the Center for Democracy and Technology, Lanny Breuer of the Justice Department and Vincent Weafer of Symantec.

<http://thehill.com/blogs/hillicon-valley/technology/77405-senate-to-hold-cybersecurity-hearing>

NIST releases update to smart grid standards

BY: JILL R. AITORO, NEXTGOV.COM
01/20/2010

The National Institute of Standards and Technology recently released the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, which provides new details on requirements for developing the smart electric grid. The document addresses the public comments from a NIST draft document that was released in September 2009 and includes new "action plans," such as "mappings between different networking technologies already in use with the grid." Mark Bellow, a spokesman for NIST, says the new guidance looks at how to accommodate technology already on the grid so that existing investments can still be used. NIST intends to finalize the smart grid cybersecurity strategy in late spring. NIST says the new guidance is "just a start" and that the framework defines how different segments of the smart grid must interact and identifies where standards are needed the most.

http://www.nextgov.com/nextgov/ng_20100120_4191.php

FBI Director to chronicle the evolution of cyber threats at RSA Conference 2010

HELP NET SECURITY
01/20/2010

Federal Bureau of Investigation Director Robert Mueller will deliver the keynote address at RSA Conference 2010, and will discuss cyber threats throughout the years from identity theft to the use of the Internet by extremists and hostile foreign powers. Mueller will also talk about the role of the FBI in addressing cybercrime and the importance of public and private sector partnerships. Sandra Toms LaPedis, area vice president and general manager of RSA Conference, said Mueller's address will provide first-hand insight into how past cyber threats have shaped our understanding of cyber warfare for the future.

<http://www.net-security.org/secworld.php?id=8734>

Is Boeing's new 747 hackable?

BY: BOB BREWIN, NEXTGOV.COM
01/20/2010

According to the Federal Aviation Administration, the computers onboard Boeing Co.'s newest version of its largest commercial aircraft, the 747-8, could allow external sources to access aircraft systems. FAA said the airliner's system architecture could "allow exploitation of network security vulnerabilities that could result in destruction, disruption, degradation or exploitation of data, systems and networks critical to the safety and maintenance of the airplane." FAA has said that Boeing must ensure electronic system security protection from unauthorized access and ensure that electronic system security threats are identified and assessed and that effective strategies are used to protect the airplane from any adverse impact on safety.

http://whatsbrewin.nextgov.com/2010/01/is_boeings_new_747_hackable.php



Keeping Cyberspace Professionals Informed

FCC looks at ways to assert authority over Web access

BY: CECILIA KANG, WASHINGTON POST
01/15/2010

The Federal Communications Commission, which currently regulates public access to telephone and television services, has been working to stake out its authority to oversee consumer access to the Internet as well. Ben Scott, director of policy at the public interest group Free Press, says the government hopes to treat broadband Internet as a national infrastructure, but federal regulators are

“grappling with older policies that do not clearly protect consumers’ access to the Web, their privacy or prices of service.” The FCC could ask Congress to grant it explicit authority over Internet service providers, but Paul Gallant, an analyst at Concept Capital, says net neutrality is a very controversial issue in the telecom media world, and would be difficult to pass.

<http://www.washingtonpost.com/wp-dyn/content/article/2010/01/14/AR2010011404717.html>

Emerging technologies.

Unpredictable threats.

Elusive enemies.

Ready for what's next. Now more than ever, mission success depends on the ability to continually adapt thinking and operations. With the perspective, experience, and know-how from battlefields and boardrooms, the strategy and technology consultants of Booz Allen Hamilton can help you achieve your cyber goals. Whether you're managing today's issues or looking beyond the horizon, count on us to help you be ready for what's next.

Booz | Allen | Hamilton
delivering results that endure

Ready for what's next. www.boozallen.com



U.S. CYBER CZAR ANNOUNCED

The cybersecurity czar's first big test

BY: KELLY JACKSON HIGGINS, DARK READING
01/14/2010

Dark Reading Senior Editor Kelly Jackson Higgins says she is waiting to see how Howard Schmidt, the nation's new cybersecurity czar, will react to the Chinese cyberattacks revealed this past week. Secretary of State Hillary Clinton has asked for an explanation of the attacks since Google went public with their accusations against the Chinese government, and a White House spokesman told the *Washington Post* that the feds are looking into the attacks. Higgins writes that Schmidt must "step in and set the agenda for that public-private partnership the administration has touted for cybersecurity." Schmidt will need to address the attacks as both an economic threat and a cybersecurity threat.

http://www.darkreading.com/blog/archives/2010/01/the_cybersecuri.html

Obama's cybersecurity czar to speak at DoD's Cyber Crime Conference

DFI NEWS
01/13/2010

Howard Schmidt, the new national cybersecurity czar, has said he will make every effort to brief attendees of the Department of Defense Cyber Crime Conference in person, via Skype or through a provided video. An exhibition during the conference will feature 70 cyber-related agencies and companies, as well as a silent auction to benefit the National Center for Missing and Exploited Children. The conference is open to federal, state and local law enforcement, as well as DoD civilians and sponsored contractors. The article also provides a list of confirmed conference session speakers. <http://www.dfinews.com/articles.php?pid=811>

NORTHROP GRUMMAN

In today's world of cybersecurity, you'll need more than a firewall to keep from getting burned.

www.northropgrumman.com/cybersecurity

▼ To really beat the bad guys, you need people not just computer programs. And Northrop Grumman has the expertise and the tools to keep your worst fears from coming true. This is the world of cybersecurity. A world we call home and know better than any other company in the industry. So when you're ready to talk to the experts about cybersecurity, come talk to us at Northrop Grumman.

THE FACE OF CYBERSECURITY.

©2009 Northrop Grumman Corporation



CYBERSPACE – DEPARTMENT OF DEFENSE (DoD)

Integrated cyber operations

BY: KEVIN COLEMAN, DEFENSE TECH
01/24/2010

Cyber attacks span the military's entire operational spectrum and offensive cyber weapons are providing commanders with new capabilities and options previously unavailable in conventional and nuclear weapons. Still, cyber weapons can be unreliable as we cannot estimate when or if an offensive cyber attack will be effective, and there is also little that can be done to control the spread of an offensive cyber attack. Cyber weapons are also dangerous because they are easy to acquire, inexpensive and able to strike at the speed of light. Cyber weapons "provide somewhat of a leveling effect" between state and non-state adversaries, terrorist groups and organized crime groups. The U.S. military must develop integrated operational strategies that can leverage our digital advantages and provide support to all aspects of our offensive, defensive and intelligence collection capabilities.

<http://defensetech.org/2010/01/24/integrated-cyber-operations/>

Cyber situational awareness

BY: KEVIN COLEMAN, DEFENSE TECH
01/18/2010

Author Kevin Coleman discusses cyber situational awareness (CSA), which involves the understanding of what is happening in a specific domain. Coleman writes that CSA is "essential for decision makers requiring changes to our decision and command infrastructure." He added that having a complete accurate CSA will require expanding the current C4ISR framework to one that includes the cyber environment. C8ISR, for example, would include command, control, communications, computers, combat systems, collaboration, coordination, code,

intelligence, surveillance and reconnaissance all adapted to the cyber warfare domain. Coleman says the U.S. military is the most computerized and modern force in the world, making the challenge of cyber situational awareness greater and more important than for any other military in the world. He concludes: "Given the current threat conditions and operations going on in the cyber domain, the adaptations of the decision making constructs will not occur in the research labs, but on the frontlines of cyber space."

<http://defensetech.org/2010/01/18/cyber-situational-awareness/>

Senior General says U.S. needs to move faster on cyber defense

BY: AL PESSIN, VOANEWS.COM
01/20/2010

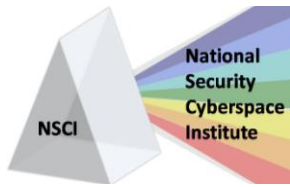
The commander of U.S. Strategic Command, Air Force Gen. Kevin Chilton, says the United States needs to do more to stay ahead of hackers and online criminals that could use malicious software to disable key American military capabilities. In addition to stepping up defense, Chilton says U.S. officials need to focus more on how to deter cyber attacks and make the consequences of an attack clear to adversaries. He explains that deterrence options could include military action, cyber counterattacks, economic retaliation and diplomatic moves.

<http://www1.voanews.com/english/news/usa/Senior-General-Says-US-Needs-to-Move-Faster-on-Cyber-Defense-82211107.html>

Air Force issues second call for network attack capabilities

BY: BOB BREWIN, NEXTGOV.COM
01/20/2010

The Air Force Electronic Systems Center says it needs industry's help in developing new ideas and technologies, as well as corrupting and



degrading information in enemy networks and information systems. Potential bidders should suggest technologies that could map an enemy's computer network, provide access to that network and help the Air Force manipulate data in enemy information systems. This solicitation, in addition to ongoing studies and acquisitions at the center, show that the Defense Department is serious about going on the offensive in cyberspace. The Electronic Systems Center is also conducting a solicitation for a Cyber Integration Environment for the Cyber Command.

http://www.nextgov.com/nextgov/ng_20100120_9002.php

Back away from GPS: AF Chief

BY: COLIN CLARK, DOD BUZZ
01/20/2010

Gen. Norton Schwartz, U.S. Air Force chief of staff, told conference attendees at Tuft University's Institute for Foreign Policy Analysis that the United States must lessen its dependence on the Global Positioning System and develop alternatives to GPS, since GPS signals are vulnerable in time of war. Air Force officials confirm that GPS satellites have been jammed and attacked recently. There are several tools that could be used to lessen the military's dependence on GPS, including digital maps and cell phone tower networks. Schwartz recommends that the United States stop building on five more GPS satellites and instead engage European allies on sharing their proposed Galileo global navigation satellite system.

<http://www.dodbuzz.com/2010/01/20/back-away-from-gps-af-chief/>

Air Force awards cybersecurity deal

UPI.COM
01/15/2010

The U.S. Air Force Research Laboratory recently chose Raytheon BBN Technologies to receive a

\$2.9 million contract to address evolving threats to the Defense Department's Service-Oriented Architectures, including the development of new applications to counter these threats. Tad Elmer, Raytheon BBN Technologies' president, says work under the new contract will "help our nation's military networks defend against the rapidly evolving variations of network and information attacks."

http://www.upi.com/Business_News/Security-Industry/2010/01/15/Air-Force-awards-cybersecurity-deal/UPI-65201263582000/

Cyber is the focus

BY: CAPT. CHRISTINA HOGGATT, AIR FORCE SPACE COMMAND PUBLIC AFFAIRS
01/14/2010

At the recent Defending America Cyberspace 2010 Symposium, Gen. C. Robert Kehler discussed the many changes in Air Force Space Command, including the 24th Air Force – a new operational command responsible for cyberspace. Kehler also discussed how the Air Force's cyber mission needs to focus more on operations instead of on communication only. He explained that the Air Force must develop "a full spectrum of capabilities within cyberspace, leveraging air and space capabilities to build a unique Air Force contribution to the joint fight." Kehler also emphasized the importance of providing training and education for cadets and Airmen entering cyberspace careers.

<http://www.af.mil/news/story.asp?id=123185516>

Army mulls realignment to fortify cyber command

BY: AMBER CORRIN, FEDERAL COMPUTER WEEK
01/15/2010

The Defense Department is reporting that Army officials are planning a unified Army cyber component that would be fully operational by October. The unit would report directly to the U.S. Cyber Command, would be headed up by a



Keeping Cyberspace Professionals Informed

three-star general and include elements of Army communications and intelligence communities. The Army Cyber Command, or ARFORCYBER, will combine all of the Army's cyber forces under a single command, integrating all aspects of network operations. <http://fcw.com/articles/2010/01/15/army-mulls-realignment-to-fortify-cyber-command.aspx>

Navy cyber forces established

BY: KATIE PACKARD, AFCEA SIGNAL MAGAZINE
01/2010

The U.S. Navy has established the Navy Cyber Forces (CYBERFOR) at the Joint Expeditionary Base, Little Creek-Fort Story in Norfolk, Va., under the command of Vice Adm. H. Denby Starling II. CYBERFOR will report to the commander for the U.S. Fleet Forces and will "organize and prioritize manpower, training, modernization and maintenance requirements; capabilities of C2 architecture and networks; cryptologic and space related systems; and

intelligence and information operations activities."

<http://www.afcea.org/signal/signalscape/index.php/2010/01/navy-cyber-forces-established/>

Poisoned PDF pill used to attack U.S. military contractors

BY: JOHN LEYDEN, THE REGISTER
01/18/2010

U.S. defense contractors recently received e-mails that appeared to be from the U.S. Department of Defense, but actually contained malicious PDF files. When the recipient opens the PDF file, the e-mail triggers an attempt to exploit an Adobe Reader vulnerability that was patched Jan. 12. If the system can be infected, the malware opens a backdoor that connects to a server in Taiwan. The new attacks prove that cyber-espionage attacks are a continuous problem.

http://www.theregister.co.uk/2010/01/18/boo-by_trapped_pdf_cyber_espionage/

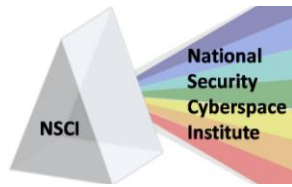


CISCO

Cisco (NASDAQ: CSCO) enables people to make powerful connections-whether in business, education, philanthropy, or creativity. Cisco hardware, software, and service offerings are used to create the Internet solutions that make networks possible-providing easy access to information anywhere, at any time. Cisco was founded in 1984 by a small group of computer scientists from Stanford University. Since the company's inception, Cisco engineers have been leaders in the development of Internet Protocol (IP)-based networking technologies.

Today, with more than 65,225 employees worldwide, this tradition of innovation continues with industry-leading products and solutions in the company's core development areas of routing and switching, as well as in advanced technologies such as: Application Networking, Data Center, Digital Media, Radio over IP, Mobility, Security, Storage Networking, TelePresence, Unified Communications, Video and Virtualization. For additional information:

www.cisco.com



'Cyber Genome Project' kicked off by DARPA

BY: LEWIS PAGE, THE REGISTER
01/26/2010

DARPA recently announced its new "Cyber Genome Project," which will "allow any digital artifact – a document, a piece of malware – to be probed to its very origins." DARPA says digital artifacts would be collected from live systems, wired or wireless networks, or collected storage media and would include electronic documents or software. The technical areas of the project will create cyber fingerprints, or DNA, which would allow scientists to "determine the identity, lineage and provenance of digital artifacts and users." The program seeks to make every document or code created traceable back to the source, just as DNA at a crime scene can be traced back to a criminal.

http://www.theregister.co.uk/2010/01/26/cyber_genome_project/

U.S. faces critical lack of (mad) computer scientists

BY: LEWIS PAGE, THE REGISTER
01/13/2010

A recent DARPA solicitation says the "downward trend in college graduates with STEM (science, technology, engineering and math) majors is particularly pronounced in Computer Science (CS)." DARPA is concerned that the United States is steadily losing the talent necessary to protect American computer systems, while computer scientists are in high demand as systems become more complex. Recent studies conducted by DARPA found that many Americans believe there are fewer computer science jobs because of the "dot-com bust" and "international outsourcing." DARPA has said it is "interested in proposals with innovative new ideas to encourage students to major in CS-STEM and pursue careers as engineers and scientists."

http://www.theregister.co.uk/2010/01/13/darpa_a_mad_scientist_base_boost_plan/

DARPA: U.S. geek shortage is national security risk

BY: KATIE DRUMMOND, WIRED BLOG NETWORK
01/15/2010

The Pentagon's research arm, DARPA, is soliciting proposals that would attract young people to careers in science, technology, engineering and math, with an emphasis on computing. The Computer Research Association reports that computer science enrollment dropped 43 percent between 2003 and 2006, making DARPA worry that America will not be able to compete without college graduates that understand and create new technologies. The organization is looking for programs that offer career days, mentoring, lab tours and counseling. DARPA plans to specifically target young women and minorities, as the decline in computer science degrees was particularly pronounced for these groups.

<http://www.wired.com/dangerroom/2010/01/darpa-us-geek-shortage-is-a-national-security-risk/>

Interview with Mark Orndorff of DISA, part I

BY: MICHAEL CHEEK, THE NEW NEW INTERNET
01/07/2010

This is the first part of an interview with Mark Orndorff, the head of the Information Assurance division of the Defense Information Systems Agency (DISA), which develops and delivers enterprise infrastructure and C&C capabilities to support modern warfighters and leaders. Orndorff answers questions about new initiatives DISA is looking to implement, some goals from the Department of Defense that DISA's IA area helps to meet and how the host-based security system plays a role in better securing DoD networks. Orndorff also discusses the balance between ensuring that joint forces



Keeping Cyberspace Professionals Informed

has access to information, while providing effective security. He says the biggest challenges are beyond joint operations, when information must be shared with coalition forces, other government or non-government organizations and outside of the DoD.

<http://www.thenewnewinternet.com/2010/01/07/interview-with-mark-orndorff-of-disa-part-i/>

Interview with Mark Orndorff of DISA, part II

BY: MICHAEL CHEEK, THE NEW NEW INTERNET
01/11/2010

This article provides the second part of an interview with Mark Orndorff, head of Information Assurance at DISA. Orndorff discusses how DISA balances privacy concerns

with effective security, and says users of DoD networks consent to monitoring, but that DISA doesn't target one individual without going through the proper legal processes. Orndorff also talks about the need for skilled IA professionals and DISA's recruitment efforts, including job fairs and an internship program that participates with several universities. DISA also offers scholarships for students that commit a certain amount of time after college to employment with the government. Finally, he discusses concerns for the information assurance field, focusing on configuration management and preventing vulnerabilities.

<http://www.thenewnewinternet.com/2010/01/11/interview-with-mark-orndorff-of-disa-part-ii/>

Assess, Detect, Respond, Secure
with a Cybersecurity Solution Built on Forensically Sound Technology

EnCase Cybersecurity

- Proactively identify and recover from covert network threats and classified spillage
- Detect polymorphic malware over the network
- Ensure endpoints remain in a trusted state

Delivering cybersecurity and forensic solutions to government agencies for more than 10 years.
Learn More >>> visit www.guidancesoftware.com or call 1-866-973-6577

Guidance SOFTWARE
The World Leader in Digital Investigations



CYBERSPACE – INTERNATIONAL

Iran accuses U.S. of using Internet against it

BY: REZA DERAKHSHI, MSNBC
01/26/2010

Following U.S. Secretary of State Hillary Clinton's remarks on ending Internet censorship, Iran's supreme leader has accused the United States of trying to use the Internet as a tool to confront the Islamic Republic. Iranian government officials say the United States supported protests that erupted during the Iranian election to undermine Iran's Islamic system of government. Supreme Leader Ayatollah Ali Khamenei says the United States is frustrated because "they have allocated a \$45 million budget to help them to confront the Islamic Republic of Iran via the Internet" but that the U.S. has "achieved no results." Iran believes that the United States is waging a "soft war" against Iran. Khamenei identifies Israel and the United States as Iran's most hostile enemies, but says that all of "America's plots and efforts during the past 30 years were fruitless."

http://www.msnbc.msn.com/id/35082205/ns/technology_and_science-security/

More cyberattacks likely from group that took down Chinese search engine

BY: JILL R. AITORO, NEXTGOV.COM
01/13/2010

The same hacking group that took down Twitter in December recently attacked China's most popular search engine, Baidu.com, taking it offline for almost four hours. In both attacks, the hackers changed the sites' DNS settings to redirect visitors to a Web page showing an Iranian flag and a message from the Iranian Cyber Army. Johannes Ullrich, chief technology officer for the SANS Institute Internet Storm Center, says the attack is actually pretty simple and may just be "some kids having fun,"

although other security experts say it isn't just an "accident that two of the top 15 most visited domains in the world were targeted in the span of a few weeks."

http://www.nextgov.com/nextgov/ng_20100113_2896.php

Why the 'China virus' hack at U.S. energy companies is worrisome

BY: JOHN YEMMA, THE CHRISTIAN SCIENCE MONITOR
01/26/2010

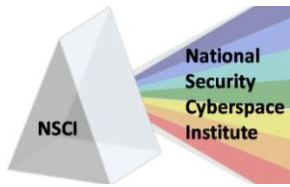
A Christian Science Monitor investigative report reveals how hackers were able to infiltrate the networks of three U.S. energy companies, targeting information that would give them valuable information on oil and gas exploration. U.S. energy companies spend hundreds of millions of dollars each year on "exploration," searching for oil and gas. Hackers are able to steal information about the most promising locations from energy companies, allowing them to easily outbid U.S. companies and save millions on exploration costs. Anti-virus software firm McAfee estimates that \$1 trillion was stolen from companies and individuals through the Internet in 2008, and that the cost could be much worse if relations between China and the U.S. deteriorate.

<http://www.csmonitor.com/Commentary/editors-blog/2010/0126/Why-the-China-virus-hack-at-US-energy-companies-is-worrisome>

Information warfare: South Korea is at war

STRATEGY PAGE
01/18/2010

In addition to the creation of South Korea's new Cyber War Center, South Korea is forming a cyber police force to protect commercial and government organizations from hackers. The new force is part of the National Intelligence Service and has already hired 3,000 Internet



security experts to work with Internet crime victims, coordinate the efforts of government agencies and develop methods for improving online security. South Korean officials report that attacks on their networks were up 20 percent last year, and claim that the majority of those attacks can be traced back to North Korean locations. South Korean intelligence reports that North Korea has a unit of at least 100 hackers that focus on scouting out South Korean government and military networks. <http://www.strategypage.com/htmlw/htiw/articles/20100118.aspx>

South Korea sets up cyberwarfare unit to repel NORK hackers

BY: JOHN LEYDEN, THE REGISTER
01/12/2010

South Korea recently launched a cyberwarfare command centre that will focus on fighting hacking attacks blamed on North Korea and China. The division includes 200 workers who will tackle the reported 95,000 daily hacking attacks on South Korean military networks, such as a recent attack where North Korea is blamed for stealing a secret U.S.-South Korean war plan from South Korean systems. Some experts believe that South Korea's new cyber command may have been formed in response to reports about a cyberwarfare unit in North Korea. http://www.theregister.co.uk/2010/01/12/korea_cyberwarfare_unit/

Gates looks to India for cyber cooperation

BY: JACK MANN, THE NEW NEW INTERNET
01/21/2010

U.S. Secretary of Defense Robert Gates was recently in Pakistan and India, hoping to increase cooperation between the two nations and the United States in a number of areas, including cyber security. U.S. officials reportedly hope to increase ties to India in the field of cyber security in order to enhance U.S. security

efforts, and because India is seen as a "countering force in Asia to Chinese influence." <http://www.thenewnewinternet.com/2010/01/21/gates-looks-to-india-for-cyber-cooperation/>

Information warfare and Indian national security

ITVOIR.COM
01/15/2010

This article discusses the need for critical infrastructure protection in India and says that "cyber war capabilities should be an integral part of Indian national defense and security." Praveen Dalal, managing partner of Perry4Law and the leading techno-legal expert in India, says the nation "needs a sophisticated and robust technological command centre to defend its global network of computer systems." Dalal says India needs to develop offensive and defensive capabilities to meet the growing threats from cyber warfare. <http://www.itvoir.com/portal/boxx/modules/bl ogs/Blog-Detail.asp?BlogID=19582>

China hackers tried to hit India, Times says

BY: JOHN RIBEIRO, TECHWORLD
01/19/2010

India's National Security Advisor M.K. Narayanan reports that his office and other government offices in India were recently targeted by hackers believed to be from China. The attacks took place Dec. 15, the same day that many U.S. companies reported they were attacked. Google has said the attacks in December were sophisticated and targeted, and that they believe the attacks originated in China. The attack on India came through e-mails with a malicious PDF attachment that contained a Trojan virus, allowing the hacker to access a computer remotely and download or delete files. <http://news.techworld.com/security/3210518/c hina-hackers-tried-to-hit-india-times-says/>



Chinese hackers target PMO

INDIA TODAY

01/14/2010

Hackers from China reportedly targeted computers in the Indian Prime Minister's Office in December. A spokesperson from the prime minister's office says no classified information had been breached, and that the PMO has its own system in place for protecting against hacking attempts. Strategic affairs analyst Bharat Karnad says China "doesn't believe in peacetime" and that "for China, it's always rivals, always competition." R.S.N. Singh, a former RAW officer, says China wants to dominate cyberspace, a very serious concern because of the harmful potential of cyber attacks. Investigators report that the Chinese hackers may have had help from within the Indian establishment, and that the espionage attempt was highly evolved and well-researched.

<http://indiatoday.intoday.in/site/Story/79215/India/Chinese+hackers+target+PMO.html>

Australia recruits cybersecurity experts

SPACEWAR

01/21/2010

The Australian Ministry of Defense has announced it will recruit an additional 130 cybersecurity experts within the next five years to join the 51 workers currently at its new operations center. Defense Minister John Faulkner says cybersecurity is one of the government's top national security priorities, and that the new center will compliment the DSD's role as the Australian authority on information security by providing the government with security advice and assistance. Critics of the Australian government claim that the country has been too slow to boost cybersecurity work.

http://www.spacewar.com/reports/Australia_recruits_cybersecurity_experts_999.html

Cyber warfare HQ opens its doors

BY: PETE VENESS, MSN

01/15/2010

Defence Minister John Faulkner recently opened the Australian Defence Signals Directorate to the media and discussed cyberwarfare and the threat to Australia's national security and national interests from cyber intrusions on government and critical infrastructure networks. Attorney-General Robert McClelland says cyber threats come from many different sources, including individuals, issue-motivated groups, organized crime groups and state-based adversaries, but the anonymous nature of the Internet makes it difficult to attribute the source of cyber incidents. Faulkner says the Cyber Security Operations Centre is expected to grow from 51 workers to 130 over the next five years.

<http://news.ninensn.com.au/national/1000120/media-allowed-peek-at-cyber-warfare-hq>

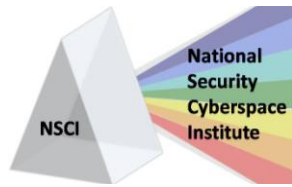
UK warfare debate

FINANCIAL TIMES

01/21/2010

The heads of Britain's Army and Royal Navy have reportedly engaged in a public argument about the future of the United Kingdom armed forces. This article discusses how both are trying to find a balance between traditional war-fighting capabilities and new assets that "allow a nation to wage counter-insurgency." General Sir David Richards, the army chief, says the UK must face the changing nature of conflict and that aggressors are able to use cyberwarfare to wage conflict. Admiral Sir Mark Stanhope, the Navy head, says high-tech capability is important because we cannot predict the crises of the future.

http://www.ft.com/cms/s/0/1c5577e8-06c4-11df-b426-00144feabdc0.html?nclick_check=1



UK.gov dismisses Tory claims UK cyberspace is defenseless

BY: CHRIS WILLIAMS, THE REGISTER
01/15/2010

The UK Conservative party recently released their national security green paper which stated that the GCHQ's Cyber Security Operations Centre is intended to just analyze threats, and not do anything about them. The paper said the United Kingdom needs to be able to prevent attacks and needs to develop proactive and offensive cyber capabilities. The Cabinet Office, which recently set up the Office of Cyber Security (OCS) says that "it was perplexed by the claim." The Conservatives said they would set up a Cyber Threat and Assessment Centre where cyber incidents could be reported, but the Cabinet Office points out this would only replicate what was being done through the OCS. http://www.theregister.co.uk/2010/01/15/tory_cyber/

French Government calls on Internet users to abandon Internet Explorer

NEW.COM.AU
01/19/2010

Many nations, including Australia and Germany, as well as Certa, a French government agency that oversees cyber threats, are advising against using Internet Explorer. Certa warns users that most attacks are effective against Internet Explorer 6, and urges users to upgrade to Internet Explorer 8, although that version is technically still vulnerable. The Australian government suggests that users try Microsoft's temporary fixes or even consider switching to an alternate browser, although Dr. Mark Gregory, Internet security expert at RMIT University, says a rush to another browser will not help protect users, but would only give hackers a new target. The article suggests that Internet users download an alternate browser such as Firefox or Apple Safari, upgrade from IE6 and upgrade their browser's security.

<http://www.news.com.au/technology/french-government-calls-on-internet-users-to-abandon-internet-explorer/story-e6frfro0-1225821078692>

Multinational cyber defense agency to expand membership

BY: BEN IANNOTTA, C4ISR JOURNAL
01/01/2010

Turkey and Hungary are reportedly joining the seven-nation Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. The United States has also expressed interest in becoming an official member. The Centre serves as a think tank that researches cyber issues at the request of NATO, although the Centre is not funded by NATO. It is significant when new nations join because they are required to assign 3 experts to the center, providing the Centre an opportunity to expand its knowledge and pool of contacts. The cyber center conducts work in three areas: legal issues, education and concepts. <http://www.c4isrjournal.com/story.php?F=4423331>

Russian hackers jam automobile traffic with porn

FOX NEWS
01/15/2010

Russian hackers were able to post a pornographic clip on a billboard in Moscow. Panno.ru operates billboards in Moscow and said hackers were behind the "graphic sex video broadcast" on two roadside screens along Moscow's Garden Ring Road. Panno.ru commercial director Viktor Laptev says the attack could have resulted from competition on the advertising market or simple "hooliganism." The clip reportedly ran for 20 minutes on the giant screen before the screen could be shut off, bringing traffic to a halt. <http://www.foxnews.com/scitech/2010/01/15/russian-hackers-jam-automobile-traffic-porn/>



GOOGLE VS. CHINA

Hacking risks persist even if firms leave

China

BY: JEREMY KIRK, COMPUTERWORLD
01/13/2010

Following Google's announcement that it may stop doing business in China because of recent cyber attacks, Whit Andrews, lead Google analyst for Gartner, says "My sense is that there would be relatively no major impact on Google's ability to defend itself based on whether it has business operations in China or not." Other experts agree that "the distributed nature of the Internet means Google and other enterprises are at no less risk from hackers sympathetic to Chinese policy by not doing business in that country." Scott Borg, director and chief economist for the U.S. Cyber Consequences Unit, says anyone who does a little e-work can achieve anonymity on the Internet, and that hackers will always have time to exploit vulnerabilities before patches are developed and released. Andre DiMino, co-founder of Shadowserver, says there will never be a day when software is completely free of vulnerabilities.

http://www.computerworld.com/s/article/9144342/Hacking_risks_persist_even_if_firms_leave_China?taxonomyId=17

China's cyberwar goes beyond Google

BY: TIM STEVENS, GUARDIAN.CO.UK
01/13/2010

This article discusses whether Google's decision to withdraw operations from China is actually because of ethical concerns, considering Google entered a censorship agreement in 2006 as a precondition for operations in China. Still, some believe that Google may not want to be associated with censorship anymore. The article also discusses efforts of the Chinese government to encourage its citizens' self-

ensorship and China's development and sponsorship of offensive cyber capabilities. Security experts generally agree that China outsources hacking activities to its citizens so that the government can deny involvement in attacks.

<http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/13/google-china-cyber-war-security>

Google: Doing the right thing

BY: LEE GOMES, FORBES
01/13/2010

Google claims that China-based hackers were responsible for trying to break into the Gmail accounts of Chinese activists, that Google will no longer censor search information on its Chinese site and may even leave the country completely. The Chinese government says it doesn't censor any information other than what is necessary to protect its citizens from criminals, terrorists and hackers. This article applauds Google for its decision to pull operations out of China, calling it a "moment of moral clarity."

<http://www.forbes.com/2010/01/13/censorship-hackers-china-technology-breakthroughs-google.html>

China won't yield to Google on censorship, analysts say

BY: OWEN FLETCHER, NEW YORK TIMES
01/13/2010

Analysts say Google is risking having its online services blocked in China if it makes good on its threat to end censorship of search results on its Chinese search engine. Danny O'Brien, an international coordinator at the Electronic Frontier Foundation, says China will likely "throw Google out, and it will undoubtedly block Google.cn," and other analysts believe



that all Google services will be blocked including Gmail, Google Docs and Google hosting for businesses. Leslie Harris, president of the Center for Democracy and Technology, praises Google for its decision to end its censorship, although some believe Google is just looking for an excuse to get out of China after losing market share to domestic rival Baidu.com. Analysts wonder if Google will make more money in China if they choose to stay.

<http://www.nytimes.com/external/idg/2010/01/13/13idg-china-wont-yield-to-google-on-censorship-analysts-sa-91824.html>

Security experts dissect Google China attack

BY: JOHN LEYDEN, THE REGISTER
01/14/2010

Security experts are surprised that Google has threatened to stop operations in China following a cyber attack on Google's systems traced to Chinese IP addresses. Many experts agree that the hackers were trying to gain access to e-mail accounts of civil rights activists and that the starting point of the attack was either sending e-mails that contained malware to Google employees or an exploitation of a vulnerability in Google's Web servers. Investigations into the attacks found that the attack affected 33 additional companies, and the IP addresses used in this attack are on the same subnet as IP addresses involved in attacks on 100 IT firms last summer, which could indicate that the same hackers are responsible for both attacks.

http://www.theregister.co.uk/2010/01/14/google_china_attack_analysis/

Microsoft's Ballmer: We're staying in China

BY: JOHN FONTANA, NETWORK WORLD
01/14/2010

Steve Ballmer, Microsoft's CEO, has said that Microsoft will stay in China and "abide by the law" even though Google is considering pulling

out of China following a cyber attack on its systems. Microsoft has been operating in China since 2006 under an agreement with the Chinese government that Microsoft will purge banned topics from its Chinese search results. Ballmer did say that China's lack of intellectual property protection makes it difficult for U.S. companies to operate in China. Ballmer also discusses recent reports that a vulnerability in Microsoft's Internet Explorer played a part in the attacks against Google.

<http://www.networkworld.com/news/2010/01/1410-ballmer-china-microsoft.html>

China defends censorship after Google attack

BY: STEVEN MUFSON, WASHINGTON POST
01/15/2010

Chinese authorities are defending their policy on online censorship and are even encouraging Internet users to censor themselves in response to Google's announcement that it will stop filtering out censored information on its Chinese-based Web site. Foreign Ministry spokesman Jiang Yu says China "proscribes any form of hacking activity" and that the Chinese government encourages openness and development of the Internet. On the Web site of the State Council Information Office, cabinet spokesman Wang Chen says the Chinese government censors certain information in order to guarantee state security and the secure flow of information.

<http://www.washingtonpost.com/wp-dyn/content/article/2010/01/14/AR2010011402482.html>

A new era of Internet control

BY: RON SYNOVITZ, RADIO FREE EUROPE/RADIO LIBERTY (RFE/RL)
01/15/2010

Following Google's announcement that it would no longer censor search results on its Chinese search engine, Beijing "reasserted its right to



Keeping Cyberspace Professionals Informed

control the Internet” through “Internet management.” Silvio Waisbord, an expert on media and globalization and the director of graduate studies at George Washington University, says it is surprising that a company the size of Google would be “willing to play hard politics with the Chinese government.” Bill Echikson, a spokesman for Google, says Google is hoping to talk with Chinese authorities about the possibility of an uncensored search service in China, but that Google would close google.cn if uncensored service was impossible.

<http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?ots591=4888CAA0-B3DB-1461-98B9-E20E7B9C13D4&lng=en&id=111344>

McAfee: China attacks a ‘watershed moment’

BY: STEVEN MUSIL, CNET.COM
01/17/2010

According to McAfee Chief Technology Officer George Kurtz on his blog, the recent China-based cyber attacks on Google were a “watershed moment in cybersecurity” because it was “the largest and most sophisticated cyberattack we have seen in years targeted at specific corporations.” Kurtz said the attack is even more significant because the goal of the

attacks appears to be to steal core intellectual property. Source code was stolen from more than 30 Silicon Valley companies in the attacks, and Kurtz warns Internet Explorer users that they “face a real and present danger.”

http://news.cnet.com/8301-1009_3-10436476-83.html

China: We are biggest victim of hacking

BY: OWEN FLETCHER, TECHWORLD
01/19/2010

China is denying any role in the recent attacks against Indian government offices, and when asked about Google’s allegations that recent cyberattacks against their corporate networks originated in China, Chinese Foreign Ministry spokesman Ma Zhaoxu said Chinese companies were often hit by cyber attacks and that China itself was the biggest victim of hackers. Google has threatened to remove operations from China and plans to hold talks with China about offering uncensored search results, but Zhaoxu said he did not know if Chinese authorities had agreed to the talks. Zhaoxu also called the allegations from the Indian government “baseless.”

<http://news.techworld.com/security/3210522/china-we-are-biggest-victim-of-hacking/>



Problem. Solved.

High Tech Problem Solvers

www.gtri.gatech.edu

From accredited DoD enterprise systems to exploits for heterogeneous networks, GTRI is on the cutting edge of cyberspace technology. Transferring knowledge from research activities with the Georgia Tech Information Security Center, GTRI is able to bring together the best technologies, finding real-world solutions for complex problems facing government and industry.



Security researcher IDs China link in Google hack

BY: ROBERT MCMILLAN, COMPUTERWORLD
01/20/2010

SecureWorks researcher Joe Stewart examined the back-door Hydraq Trojan used in the attacks against Google and found that it used an unusual algorithm to check for data corruption. Stewart reports that the source code for this algorithm is only found on Chinese Web sites, suggesting that the person that wrote it reads Chinese, linking China to the recent attacks. Stewart also says that he has never seen this particular algorithm used anywhere else except with the Hydraq, which allows attackers to run commands on the computers they hack. Hackers could use the Trojan to list directories and read or search files.

http://www.computerworld.com/s/article/9146239/Security_researcher_IDS_China_link_in_Google_hack

Google suspects Honker Union to be the culprit of its recent cyber attack

BY: ED LISTON, BENZINGA
01/20/2010

Some experts believe that a Hong Ke organization, popularly called the Honker Union, is responsible for the recent attacks against Google and other U.S. corporations, although the Hong Ke people claim they only work to prevent Chinese Web sites from being hacked. Hong Ke is the name used for Chinese "interactive trainers" who teach young people how to hack and how to use hacking tools that are available online. This particular group, the Honker Union, was involved in an incident with U.S. hackers in 2001 and recently attacked Iranian Web sites in retaliation for the Iranian Cyber Army's takeover of Chinese search engine Baidu.

<http://www.benzinga.com/general/93085/google-suspects-honker-union-to-be-the-culprit-of-its-recent-cyber-attack-goog>

What's really at stake in Google vs. China

CNN
01/21/2010

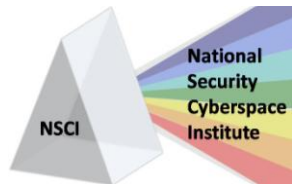
CNN interviews Fareed Zakaria, author and host of CNN's "Fareed Zakaria: GPS." Zakaria discusses the dispute between Google and China, and says that China is having a difficult time balancing its drive for modernity and attempting to control information. Zakaria says China is "turning inward" as many Chinese believe that China should be more aggressive towards the West since China's economy is growing and the nation doesn't need the United States like it once did. Zakaria also discusses the difficulty of determining whether hackers are working for the Chinese government or on their own, and whether or not the U.S. government should be more active in cyber security. Zakaria says Washington needs to have a sustained strategic dialogue with China as well as our other allies in order to create an environment of openness and greater cooperation. Finally, Zakaria says the "trillion-dollar question" is whether or not China can continue to limit the expression of different political views as its economy grows and while the Web becomes an even more important medium for communication worldwide.

<http://www.cnn.com/2010/OPINION/01/21/zakaria.google.china/>

Google didn't kowtow and neither should you

BY: JOHN BOLTON, WALL STREET JOURNAL
01/21/2010

This article discusses how Google's threat to withdraw from China has broader implications for how U.S. businesses must approach the Chinese market and for the U.S. government, "which has often failed to vigorously assert U.S. political and economic interests." The attractiveness of the Chinese market has often quieted complaints by foreign businesses and experts often urge businesses not to "press too



hard on China” which has led to nothing being done to change undesirable Chinese policies, and may have even encouraged Beijing to continue them. The article states that no business until Google has challenged the censorship policies of the Chinese government, and says “It may be China that is the paper tiger – but how will we know, if we never test it?” The article urges American businesses and the U.S. government to vigorously defend their interests in China and not to make deals out of fear of retaliation or lack of cooperation from Beijing.

http://online.wsj.com/article/SB10001424052748703699204575016422427490804.html?mod=WSJ_latestheadlines

China attacks Clinton’s Internet speech as ‘harmful’ to relations

BY: STEVEN MUFSON, WASHINGTON POST
01/22/2010

Chinese Foreign Ministry spokesman Ma Zhaoxu says that U.S. Secretary of State Hillary Clinton’s recent remarks calling for Internet freedom “insinuated that China restricts Internet freedom” and that the remarks were “contrary to the facts and harmful to China-U.S. relations.” Clinton said the Internet is linked to other basic freedoms, such as the freedom of speech, worship or assembly. Clinton added that the U.S. government would support and fund individuals and companies in countries with restricted access to find ways to circumvent obstacles. Rao Jin, founder of Anti-CNN, says Clinton’s speech will likely lead to strong resentment from the Chinese people and that China will never allow a foreign country to impose their ideologies on China.

<http://www.washingtonpost.com/wp-dyn/content/article/2010/01/22/AR2010012201090.html>

China rejects accusations on Google hack, Internet freedom

BY: OWEN FLETCHER, COMPUTERWORLD
01/24/2010

According to *Xinhua* news agency, China has dismissed accusations of any involvement in the attacks on Google and other U.S. companies, and defends online censorship of political topics. Google claims it was attacked by hackers from China that were able to steal intellectual property and access the Gmail accounts of Chinese human rights activists. Chinese officials say that Chinese law forbids hacking other countries and that they are open to international cooperation to fight cybercrime. China currently requires Google and other companies to remove certain items from search results, but Google CEO Eric Schmidt says that Google will soon stop censoring search results.

http://www.computerworld.com/s/article/9147799/China_rejects_accusations_on_Google_hack_Internet_freedom

China steps up defense of Internet controls

BY: CHRIS BUCKLEY, THE WASHINGTON POST
01/25/2010

China has recently increased its defense of Internet censorship after Google announced it would stop censoring its Chinese Google.cn Web site. Google received support from the White House, but China says Washington is using the Internet debate to support subversion in Iran. David Wolf, president of Wolf Group Asia, says this case is becoming very politically important for China, and that they cannot back down on such a fundamental issue. A spokesperson for China’s State Council Information Office says China has “ample legal basis” for blocking harmful content online, and that their policies are “completely different from so-called restriction of Internet freedom.”

<http://www.washingtonpost.com/wp-dyn/content/article/2010/01/24/AR2010012403023.html>



Keeping Cyberspace Professionals Informed

Google may keep some Chinese operations

FOX NEWS
01/26/2010

Despite Google's recent threats to close its search engine in China, Google is in talks with the Chinese government to keep its research center there. Google would also like to keep an advertising sales team in China as well as a "fledgling mobile phone business." The talks are delicate because of Google's decision to stand

up to the Chinese government over Internet censorship, but Google reportedly wants to maintain access to China's engineering talent and growing online advertising and mobile phone markets.

<http://www.foxnews.com/scitech/2010/01/26/google-chinese-operations/>

Proven Cyber Security Services and Solutions

ManTech has been providing cyber operations services to the U.S. government and private industry for 17 years and its cyber professionals are experts in the field who have authored books and articles on honeypots (catching hackers), service oriented architecture security, and network security monitoring. They have also taught for leading cyber security education providers such as SANS, Foundstone, USENIX, HTCIA and Black Hat. ManTech supports more than twenty sensitive clients in the national security and Intelligence Communities, as well as AmLaw 100 clients, federal and state agencies, and Fortune 500 corporations.

Our services include:

- Computer forensics and intrusion analysis
- Counter-intrusion support
- Penetration testing and network simulation
- Security and secrecy solutions
- Infrastructure protection
- Language support services
- Training and seminars

www.mantech.com

CYBERSPACE RESEARCH

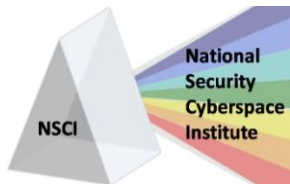
Declining confidence in social networking security

HELP NET SECURITY
01/21/2010

RSA recently released their 2010 Global Online Consumer Security Survey, which polled more than 4,500 consumers regarding their awareness of online threats and concerns with the safety of their personal information online. Nearly two out of three respondents said they

are less likely to share information on social networking sites due to growing security concerns. Four out of five people that use social networks said they are concerned with the safety of their personal information online. Despite increased awareness, the number of consumers that have fallen victim to a phishing scam increased six times in 2009.

<http://www.net-security.org/secworld.php?id=8745&utm>



Mal-Bredo A virus spreads via social media

DARK READING

01/12/2010

Commtouch recently released its Internet Threats Trend Report for Q4 2009, finding that cybercriminals are using the reputations of global brands such as UPS and Facebook to get recipients to open malicious e-mails. The Q4 Trend Report also found that spam makes up approximately 77 percent of all e-mail traffic and that "business" continues to be the Web site category most infected with malware. Pharmaceutical spam is still the most popular type of spam message and Brazil is still responsible for producing the most zombie machines. Commtouch Vice President of Products Asaf Greiner says the report shows how criminals are becoming more creative to ensure their messages are opened.

http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=222300666

Report: DDoS attacks still growing, but at slower rate

BY: KELLY JACKSON HIGGINS, DARK READING

01/19/2010

Arbor Networks recently released its annual worldwide security infrastructure report and found that the number of distributed denial-of-service attacks grew 20 percent last year – a significant decrease in the rate of attacks from 2007 to 2008, when the number of attacks increased 67 percent. Craig Labovitz, chief scientist for Arbor, says the attacks have slowed down because most data centers are no longer as susceptible to brute-force volume attacks as they were in the past, and because most service providers and large enterprises have measures in place that can address most DDoS attacks. The report did say that attackers are using smaller-scale DDoS attacks that are harder to detect more frequently.

<http://www.darkreading.com/securityservices/security/perimeter/showArticle.jhtml?articleID=222301511>

Intelligent Software Solutions



ISS is a leading edge software solution provider for enterprise and system data, services, and application challenges. ISS has built hundreds of operationally deployed systems, in all domains – "From Space to Mud"™.

With solutions based upon modern, proven technology designed to capitalize on dynamic service-oriented constructs, ISS delivers innovative C2, ISR, Intelligence, and cyber solutions that work today and in the future. <http://www.issinc.com>.

CYBERSPACE HACKS AND ATTACKS

Fearing hackers who leave no trace

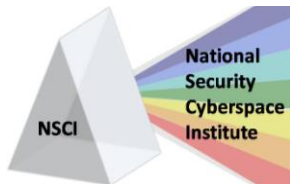
BY: JOHN MARKOFF & ASHLEE VANCE, NEW YORK

TIMES

01/20/2010

This article discusses how hackers attempt to steal a company's source code – which could

decrease the company's competitive edge in the marketplace – or change the source code, giving the hackers access to everything the company and its customers did with the software. Jeff Moss, a security expert who sits on the Homeland Security Advisory Council,



says the Adobe Systems may soon be the most targeted company in attacks, since Acrobat is installed on approximately 95 percent of all machines in the world and there have been several vulnerabilities found in Flash. Moss says that if a hacker can find a vulnerability in one of these products, they are “golden.” Hackers look at source codes of software at companies, such as Adobe, to find new ways to infiltrate products before the companies can fix software errors.

<http://www.nytimes.com/2010/01/20/technology/20code.html>

Juniper, Symantec investigating after Google attack

BY: ROBERT MCMILLAN, COMPUTERWORLD
01/15/2010

Juniper Networks and Symantec are investigating the recent cyber-espionage attacks that affected 34 companies, most of them large Fortune 500 names. The attackers used a “zero-day” attack on Internet Explorer to steal information from the companies, including Google and Adobe. Symantec and Juniper Networks have reported they are investigating the incident, but have not said if they were targeted in the attack. Google has said they believe China was behind the attacks, and James Lewis of the Center for Strategic and International Studies says this attack proves that even the biggest companies are no match for a big foreign intelligence service.

http://www.computerworld.com/s/article/9145019/Juniper_Symantec_investigating_after_Google_attack

Yahoo reportedly hit by China hackers

BY: ROBERT MCMILLAN, COMPUTERWORLD
01/14/2010

News sources are now reporting that Yahoo was one of the more than 30 companies targeted in a sophisticated cyberattack from China meant to steal intellectual property and

collect information on Chinese dissidents. Google and Adobe have already admitted to being targeted in the attacks, and more names are expected to come to light in the next few days. Yahoo has said in a statement that they are “committed to protecting human rights” and that they take user privacy and security very seriously.

http://www.computerworld.com/s/article/9144899/Yahoo_reportedly_hit_by_China_hackers

Hackers used rigged PDFs to hit Google – and Adobe, says researcher

BY: GREGG KEIZER, COMPUTERWORLD
01/13/2010

Adobe has confirmed that the recent cyberattacks that hit its corporate network earlier this month were connected to the attacks that Google reported. The attacks were reportedly based on malicious PDFs that exploited a vulnerability in Adobe’s Reader software. Adobe patched a zero-day vulnerability yesterday, although Adobe denies any link between patching the Reader flaw and the announcement that it had been attacked. Mikko Hypponen, chief research officer of F-Secure, says he and other researchers found that the attack was spread through an e-mail with an exploit-ridden PDF attachment, although there is nothing technically new in the attacks.

http://www.computerworld.com/s/article/9144378/Hackers_used_rigged_PDFs_to_hit_Google_and_Adobe_says_researcher

Verisign mistaken about Adobe flaw’s part in Google attack

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD
01/18/2010

Verisign’s iDefense security group recently released a statement, retracting their earlier assessment that attackers had exploited a vulnerability in Adobe Reader in the recent attacks against Google and other companies.



Keeping Cyberspace Professionals Informed

Verisign has since said “there are currently no confirmed instances of a vulnerability in Adobe technologies being used in these attacks.” Microsoft recently confirmed that an unpatched vulnerability in Internet Explorer software was actually used during the attack, and has issued a security warning to IE users.
<http://news.techworld.com/security/3210434/verisign-mistaken-about-adobe-flaws-part-in-google-attack>

DIY cybercrime kits power growth in Net phishing attacks

BY: BYRON ACOHIDO, USA TODAY
01/17/2010

Do-it-yourself cybercrime kits have been dropping in price and are now more user-friendly, prompting a surge in Internet-borne computer infections. Cyber criminals are using the DIY kits to carry out phishing campaigns capable of sending large amounts of fake e-mail messages that appear to be official messages from UPS, the IRS, Facebook, Microsoft Outlook or medical alerts. When the recipient clicks on a link in the malicious e-mail, their machine is infected with a banking Trojan designed to steal financial account login information. Kits usually range from \$400 to \$700 and make it easy to distribute malware, causing an increase in

Internet infections and the discovery of unique banking Trojans.
http://www.usatoday.com/tech/news/computersecurity/2010-01-17-internet-scams-phishing_N.htm

IE attack code out in the open

BY: ROBERT MCMILLAN, TECHWORLD
01/17/2010

The Internet Explorer attack code used in last month’s attack on Google’s corporate networks was recently submitted for analysis on the Wepawet malware analysis Web site, making the code publicly available. The code has already been released in a public hacking tool and is expected to be seen in future attacks, according to Dave Marcus, director of security research and communications at McAfee. Microsoft has issued a security advisory on the IE flaw and security researchers expect Microsoft to release an emergency out-of-cycle patch to fix the flaw. Germany’s federal IT security agency, the Federal Office for Information Security, has even advised users to use an alternative browser until Microsoft releases a patch.
<http://news.techworld.com/security/3210400/ie-attack-code-out-in-the-open/>

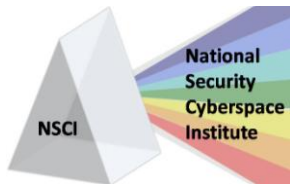
You need to focus on dozens of tasks each second in order to keep information operations at full speed. Being concerned about the security of your information shouldn't be one of them. Whether your mission is to secure information from a crime scene or prevent network intrusions, ITT makes it our mission to relieve that concern. We provide the most comprehensive suite of tools available to ensure that your information arrives at its destination, without compromising data integrity and timeliness. Learn more at aes.itt.com.

In the world of information security, second place is not an option.



Communications • Sensing & Surveillance • Space • Advanced Engineering & Integrated Services

ITT, the Engineered Blocks logo, and ENGINEERED FOR LIFE are registered trademarks of ITT Manufacturing Enterprises, Inc., and are used under license. © 2009, ITT Corporation.



Whirlpool's Kitchenaid.com remains malware infected for 5 months

CYBERINSECURE.COM

01/25/2010

United Kingdom anti-virus firm Sophos claims that it tried for months to clean up Whirlpool's Kitchenaid.com Web site without success, before publicly announcing that the site remains infected with the Badsrc-C (Asprox) strain of malware. Senior Sophos Threat Analyst Paul Baccas says several people from Sophos have tried to talk to contacts at Whirlpool, but all have "consistently hit brick walls." The Asprox strain of malware found on the Kitchenaid.com site has been linked to phishing scams in the past, although the malicious script on the Kitchenaid site currently points to nowhere.

<http://cyberinsecure.com/whirlpools-kitchenaidcom-remains-malware-infected-for-5-months/>

iPhone hacker says he's also cracked PlayStation 3

BY: ROBERT MCMILLAN, NETWORK WORLD

01/25/2010

In a recent blog post, 20-year-old hacker George Hotz said he is able to run his own software on the PlayStation 3, which should only be able to play digitally-signed software approved by Sony. Hotz received widespread media attention in 2007 when he hacked the iPhone, enabling it to run on any wireless network. Hotz's newest hack could allow PlayStation 3 users to run unauthorized software on their systems, including Playstation 3 games or pirated software.

<http://www.networkworld.com/news/2010/01/2610-iphone-hacker-says-hes-also.html>

Unknown computer virus hits University of Exeter network in UK

CYBERINSECURE.COM

01/21/2010

The United Kingdom's University of Exeter's computer networks were reportedly hit with a virus that is affecting systems running Microsoft Windows Vista with Service Pack 2. David Allen, the university's registrar and deputy chief executive, says the university had to shut down their entire network in order to isolate the virus that was corrupting data. Insider sources say the virus has not been seen before and that there is no fix available. Graham Cluley, senior technology consultant at Sophos, explains that university IT teams can have a tough time securing networks, since so many students plug their own devices into the network and many show little concern for the security of a communal computer.

<http://cyberinsecure.com/unknown-computer-virus-hits-university-of-exeter-network-in-uk/>

Hundreds of Network Solutions sites hacked

BY: BRIAN KREBS, KREBSONSECURITY.COM

01/19/2010

Web site domain registrar and hosting provider, Network Solutions, reports that hackers broke into their servers and were able to deface hundreds of customer Web sites. The hackers replaced the sites' content with anti-Israeli sentiments and pictures of militants armed with rocket launchers and rifles. There may be thousands of sites affected. Network Solutions said hackers used a "file-inclusion" weakness in the company's Unix servers to get in. They also said there was no danger to customers' private or secure information.

<http://www.krebsonsecurity.com/2010/01/hundreds-of-network-solutions-sites-hacked/>



Microsoft perform DOS on Perl Testers


THE H SECURITY

01/16/2010

According to a blog post from the Perl CPAN Testers, the CPAN Testers' server has been scanned by 20 to 30 Microsoft botnets every few seconds as part of a denial-of-service attack, making it difficult for the CPAN Testers to access their sites, databases and mirrors. The IP addresses of the bots were identified as coming from Microsoft, and the administrators

of CPAN Testers has blocked access to the site from these IP addresses. The bots ignore the rules specified in robots.txt, which tells the bots what is safe to scan and what should be ignored.

<http://www.h-online.com/security/news/item/Microsoft-bots-perform-denial-of-service-on-Perl-Testers-906094.html>



The Center for Terrorism Law is hosting a conference entitled: **Cyber Security - Legal and Policy Issues for National Security, Law Enforcement and Private Industry**. This event will be held at St. Mary's University School of Law, March 18-19, 2010. For more information, please call Faithe Campbell at (210) 431-2219, or visit the Center for Terrorism Law website at www.stmarytx.edu/ctl.

CYBERSPACE TACTICS AND DEFENSE

Gmail ups security after Chinese attack

BY: CHARLES ARTHUR, GUARDIAN.CO.UK

01/13/2010

Google recently announced that Gmail will now be encrypted by default as a guard against hackers. Google says they initially left the decision up to users because https can make mail slower, but ultimately decided to turn on https for everyone to protect data from being snooped on.

<http://www.guardian.co.uk/technology/2010/jan/13/gmail-increases-security-chinese-attack>

SAIC to acquire CloudShield

DARK READING

01/15/2010

Science Applications International Corporation (SAIC) recently announced it has signed a definitive agreement to acquire CloudShield Technologies, Inc. – a cybersecurity and management solutions provider. CloudShield provides a deep packet inspection (DPI) platform, consisting of computer hardware, secure operating systems, application development environments and numerous applications that enable their customers to inspect, analyze and control all network traffic. The acquisition will allow SAIC to bring to market DPI solutions for high speed networks,



meeting emerging requirements in U.S. federal government and commercial markets. Matt Jones, CEO of CloudShield, says the company looks forward to “combining technologies, services and expertise that will enable us to develop more robust solutions for current and future customers.”

<http://www.darkreading.com/security/management/showArticle.jhtml?articleID=222301224>

Lockheed Martin invests in cyber security talent and workforce development

DARK READING
01/20/2010

Lockheed Martin recently announced it would increase its workforce development initiatives designed to target certified and trained cyber security workers. Lockheed Martin’s commitment includes the implementation of a Cyber University; university recruiting; cyber career paths; mentoring; knowledge transfer and competitive compensation. Lockheed Martin has also awarded new academic graduate scholarships to students at Carnegie Mellon, Purdue University and the University of Maryland. Lockheed Martin plans to recruit cyber workers they can train and put on an established career track. The Lockheed Martin Cyber University provides cyber training and certification, including CISSP certification, Security + and technology training from Cisco and McAfee.

<http://www.darkreading.com/security/government/showArticle.jhtml?articleID=222301688>

JavaScript hack enables flash on iPhone

BY: CHARLIE SORREL, WIRED BLOG NETWORK
01/14/2010

Programmer Tobias Scheider has “managed to get the iPhone to run interactive apps created using Adobe’s Flash platform” by creating software, called Gordon, that works in the Safari browser and isn’t subject to the dictatorial rules of Apple’s App Store. The

Gordon software is a JavaScript runtime which allows the browser to play and display .swf files, although it doesn’t actually allow Flash to work on the iPhone. The software could open the door for new interactive and animated mobile Web sites. The lack of Flash support has been one of the most persistent criticisms of the iPhone platform, and the Adobe workaround has given developers a way of converting Flash apps to iPhone apps, although those apps would still be subject to Apple’s approval before they are made available.

<http://www.wired.com/gadgetlab/2010/01/hack-enables-flash-on-iphone/>

How not to deploy SSL

BY: KELLY JACKSON HIGGINS, DARK READING
01/15/2010

Although there were several high-profile hacks last year, demonstrating the weakness of Secure Sockets Layer (SSL), this article discusses mistakes that organizations make when deploying SSL that makes them more vulnerable to attacks. In a presentation at the OWASP meeting in London, Ivan Ristic, a researcher with SSL Labs, listed mistakes organizations make when deploying SSL, including self-signed SSL certificates; do-it-yourself certificate authorities; mixing SSL and plain text; not using secure cookies; using incomplete certificates; not using EV SSL; not using SSL at all; mixing page content; poor Web site management; only using SSL for certain parts of a site; and inconsistent DNS configuration. Ristic explains how each of these mistakes can leave SSL open and vulnerable to hackers.

http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=222301193



Thales, Voltage Security to deliver End-to-End Encryption, key management solutions

SECURITY PARK

01/21/2010

Thales and Voltage Security, Inc., recently announced a partnership that centers around delivering End-to-End Encryption and key management solutions for the payments industry and enterprise security applications. The two companies have integrated Voltage SecureData technology with Thales hardware security modules (HSMs). While End-to-End Encryption is the current leading method of securing data for organizations subject to PCI DSS, using hardware security modules solutions can further reduce the scope of PCI audits, saving time and money required for compliance. The technology integration allows customers to better secure data without having to make expensive changes to the point of sales infrastructure, database and business applications.

http://www.securitypark.co.uk/security_article_264243.html

Hackers are defeating tough authentication, Gartner warns

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD

01/18/2010

A report from Gartner Inc. says passwords and phone-based user authentication are no longer enough to protect online banking systems against fraud, as cybercriminals are developing more sophisticated ways of stealing banking log-in credentials. Trojan horse programs inside a customer's Web browser, for example, can steal passwords and have funds transferred. When banks use a phone-based authentication system, criminals can use call forwarding so the fraudster receives calls from the financial institution, instead of the legitimate customer. Security experts warn banks to use server-based fraud detection to monitor transactions for suspicious activity or differences between online banking transaction patterns and a customer's usual behavior.

http://www.computerworld.com/s/article/34633/User_Authentication_No_Longer_Thwarts_Online_Bank_Thieves

CYBERSPACE - LEGAL

Google-China row spurs on cyber bill

BY: ERIC CHABROW, GOVINFOSECURITY.COM

01/14/2010

Sen. Jay Rockefeller (D-W.Va.) says he plans to get committee approval of his cybersecurity bill, S 773, in the next few months because of the increasing number of cyber attacks, such as the recent attacks on Google that appear to have come from China. Rockefeller says this latest attack shows how our nation's public and private infrastructure is vulnerable and unprotected. There are currently 18 cybersecurity bills before Congress, but Rockefeller's bill has received much attention because of a provision that would give the president the power to shut down Internet

traffic to government sites in the case of an emergency. Rockefeller's bill would also promote public awareness about cybersecurity, create a partnership between government and the private sector on cybersecurity and foster innovation in cybersecurity in order to develop long term security solutions.

http://www.govinfosecurity.com/articles.php?art_id=2078

McKinnon wins review of extradition for hacking

BY: IAN GRANT, COMPUTER WEEKLY

01/13/2010

Hacker Gary McKinnon has been granted a reprieve from extradition to the United States,



where he could be given up to 70 years in jail for hacking federal and Pentagon computers. McKinnon suffers from Asperger's syndrome and is said to be suicidal because of the legal process. McKinnon does admit to hacking the systems, but denies causing the damage that is claimed by the United States. Judge Justice Mitting had to consider whether to refuse to surrender McKinnon under Section 8 of the Human Rights Act, or whether new evidence on the hacker's condition constituted a change in circumstances previously considered by the Home Secretary. Mitting said both issues were arguable and that if the answer to both was affirmative, the Home Secretary's decision to extradite McKinnon may be unlawful.

<http://www.computerweekly.com/Articles/2010/01/14/239946/McKinnon-wins-review-of-extradition-for-hacking.htm>

Law firm in Green Dam suit targeted with cyberattack

BY: ROBERT MCMILLAN, COMPUTERWORLD
01/13/2010

Gipson Hoffman & Pancione, the law firm representing U.S. software company Cybersitter in a legal dispute over China's Green Dam censorship software, reports it was recently targeted in a sophisticated cyber attack similar to the one reported by Google. Although 10 employees were targeted with e-mails that appeared to come from within the company, the employees had been warned to look out for

suspicious e-mails and none followed the links or attachments in the messages. Gipson Hoffman & Pancione may have been targeted because the firm is representing Cybersitter in a \$2.2 billion copyright infringement lawsuit against the Chinese government, in which Cybersitter believes the Chinese censoring software, Green Dam, uses about 3,000 lines of its Internet content filtering code.

http://www.computerworld.com/s/article/9144618/Law_firm_in_Green_Dam_suit_targeted_with_cyberattack

Nebraskan pleads guilty to 2008 Web attack on Scientologists

BY: SUMNER LEMON, COMPUTERWORLD
01/26/2010

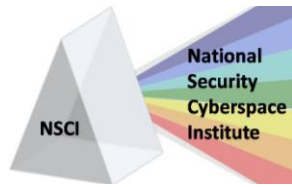
Brian Thomas Mettenbrink of Grand Island, Neb., will plead guilty to charges of unauthorized access of a protected computer for his involvement in a January 2008 attack on Web sites of the Church of Scientology. The U.S. Department of Justice reports that Mettenbrink will serve a one-year prison sentence as part of his plea. Mettenbrink admits that he downloaded software from an Internet message board that he used to help overwhelm Scientology Web sites.

http://www.computerworld.com/s/article/9148698/Nebraskan_pleads_guilty_to_2008_Web_attack_on_Scientologists?source=rss_security

Raytheon

Raytheon

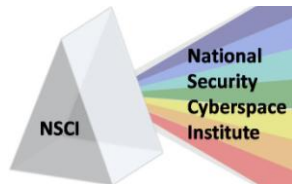
Aspiring to be the most admired defense and aerospace systems supplier through world-class people and technology Raytheon is a technology leader specializing in defense, homeland security, and other government markets throughout the world. With a history of innovation spanning more than 80 years, Raytheon provides state-of-the-art electronics, mission systems integration, and other capabilities in the areas of sensing; effects; command, control, communications and intelligence systems, as well as a broad range of mission support services.



CYBERSPACE-RELATED CONFERENCES

Note: Dates and events change often. Please visit web site for details. Please provide additions, updates, and/or suggestions for the CYBER calendar of events [here](#).

02 – 03 Feb 2010	2010 Cyber Security Expo , Washington D.C.; http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LT7G
02 – 04 Feb 2010	Information Assurance Exposition , Nashville, TN; http://www.informationassuranceexpo.com/emailtemplates/IAE_Email-Template2.html?utm_source=MailingList&utm_medium=email&utm_campaign=IAE+Booth+Sales+%26+Sponsorships+Available
05 – 07 Feb 2010	SchmooCon 2010 , Washington, DC; http://www.shmoocon.org/
11 Feb 2010	AFEI Security in the Clouds , Alexandria, VA; http://www.afei.org/events/OA02/Pages/default.aspx
17 – 18 Feb 2010	7th Annual Worldwide Security Conference , Brussels, Belgium; http://www.conferencealerts.com/seeconf.mv?q=ca1m3m8x
18 – 19 Feb 2010	Information Assurance – Latest Requirements and Methods , San Diego, CA; http://www.ttcus.com/view-seminar.cfm?id=88
25 – 26 Feb 2010	Current and Future Military Data Links , San Diego, CA; http://www.ttcus.com/view-seminar.cfm?id=89
25 – 26 Feb 2010	Information Assurance – Latest Requirements and Methods , Las Vegas, NV; http://www.ttcus.com/view-seminar.cfm?id=88
28 Feb – 03 Mar 2010	NDSS Symposium 2010 , San Diego, CA; http://www.isoc.org/isoc/conferences/ndss/10/cfp.shtml
01 – 05 Mar 2010	RSA Conference , San Francisco, CA; http://www.rsaconference.com/index.htm
03 – 05 Mar 2010	Secure IT 2010 Conference , Los Angeles, CA; http://www.secureitconf.com/
12 – 14 Mar 2010	5th Global Conference: Cybercultures – Exploring Critical Issues , Salzburg, Austria; http://www.conferencealerts.com/seeconf.mv?q=ca1mx666
18 – 19 Mar 2010	Cyber Security - Legal and Policy Issues for National Security, Law Enforcement and Private Industry , San Antonio, TX; http://www.stmarytx.edu/ctl/index.php?site=centerForTerrorismLawCyberSecurity
22 – 26 Mar 2010	USMC Annual Information Assurance Conference 2010 , Temecula, CA; http://www.technologyforums.com/10MC/
23 – 24 Mar 2010	GovSec and U.S. Law Conference , Washington DC; http://www.govsecinfo.com/Home.aspx
23 – 24 Mar 2010	Cyber Security: Missions, Initiatives, Opportunities and Risks , Washington D.C.; http://ttcus.com/view-about.cfm?id=135
23 – 25 Mar 2010	FISSEA Conference 2010 , Gaithersburg, MD; http://csrc.nist.gov/organizations/fissea/home/index.shtml
23 – 25 Mar 2010	FOSE , Washington, DC; http://www.fose.com/Events/FOSE-2010/Home.aspx
24 – 25 Mar 2010	ICIW 2011: 6th International Conference on Information Warfare and Security , Washington D.C.; http://www.academic-conferences.org/icwi/icwi-future.htm
26 – 28 Mar 2010	EuroForensics Conference , Istanbul, Turkey; http://euroforensics.com/
29 – 30 Mar 2010	Information Assurance – Latest Requirements and Methods , Washington, DC; http://www.ttcus.com/view-seminar.cfm?id=88
30 – 31 Mar 2010	AFCEA Belvoir Industry Days 2010 , National Harbor, MD; http://fbcinc.com/event.aspx?eventid=Q6UJ9A00L29J
07 – 08 April 2010	9th Annual Security Conference , Las Vegas, NV; http://www.security-conference.org/



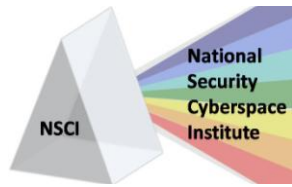
08 – 09 April 2010	5th International Conference on Information Warfare and Security , Wright-Patterson Air Force Base, Ohio; http://academic-conferences.org/iciw/iciw2010/iciw10-home.htm
12 – 14 April 2010	7th International Conference on Information Technology , Las Vegas, NV; http://www.itng.info/
12 – 14 April 2010	Security 2010 , Atlanta, GA; http://net.educause.edu/sec10
12 – 15 April 2010	European Wireless 2010 , Lucca, Italy; http://www.ew2010.org/
13 – 15 April 2010	9th Symposium on Identity and Trust on the Internet (IDTrust 2010) , Gaithersburg, MD; http://middleware.internet2.edu/idtrust/2010/
20 April 2010	NIST IT Security Day , Gaithersburg, MD; http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LN9J
20 – 22 April 2010	Tactical G4 Conference 2010 ; Atlanta, GA; http://www.technologyforums.com/10FO/
22 – 23 April 2010	Information Assurance – Latest Requirements and Methods , Washington, DC; http://www.ttcus.com/view-seminar.cfm?id=88
23 April 2010	Social Networking in Cyberspace , Wolverhampton, UK; http://www.conferencealerts.com/seeconf.mv?q=ca1mhm38
27 – 29 April 2010	Phoenix Challenge 2010 Conference , Dayton, OH; https://www.phoenixchallengeconf.org/
03 – 07 May 2010	2010 DISA Customer Partnership , Nashville, TN; http://www.disa.mil/conferences/2010/index.html
04 – 08 May 2010	Mobile Forensics World , Chicago, IL; http://www.mobileforensicsworld.com/
16 – 19 May 2010	31st IEEE Symposium on Security and Privacy , Oakland, CA; http://oakland31.cs.virginia.edu/index.html
17 – 18 May 2010	Cyber Defense: National Security in a Borderless World , Tallinn, Estonia; http://www.smi-online.co.uk/events/overview.asp?is=1&ref=3242
24 – 27 May 2010	CEIC , Las Vegas, NV; http://www.ceicconference.com/
06 – 09 June 2010	Techno Security & Digital Investigations Conference , Myrtle Beach, SC; http://www.techsec.com/
13 – 18 Jun 2010	22nd Annual FIRST Conference , Miami, FL; http://conference.first.org/About/overview.aspx
16 – 18 June 2010	Conference on Cyber Conflict , Tallinn, Estonia; http://www.ccdcoe.org/conference2010/
21 – 25 Jun 2010	TechConnect World Conference & Expo , Anaheim, CA; http://www.techconnectworld.com/
01 – 02 July 2010	9th European Conference on Information Warfare and Security , Thessaloniki, Greece; http://academic-conferences.org/eciw/eciw2010/eciw10-home.htm
14 – 16 July 2010	Symposium on Usable Privacy and Security , Redmond, WA; http://cups.cs.cmu.edu/soups/2010/
17 July 2010	Cyberpsychology and Computing Psychology Conference (CyComp 2010) , Bolton, Lancashire, UK; http://www.conferencealerts.com/seeconf.mv?q=ca1mxia6
26 – 28 July 2010	Secrypt 2010 , Athens, Greece; http://secrypt.icete.org/



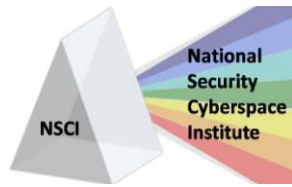
CYBERSPACE-RELATED TRAINING COURSES

Note: Dates and events change often. Please visit web site for details. Please provide additions, updates, and/or suggestions for the CYBER calendar of events [here](#).

Certified Ethical Hacker	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=10463&catid=191&country=United+States
Certified Secure Programmer (ECSP)	EC-Council, Online, http://www.eccouncil.org/Course-Outline/ECSP.htm
Certified VoIP Professional	EC-Council, Online, http://www.eccouncil.org/Course-Outline/ECVP.htm
CISA Prep Course	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=9416&catid=191&country=United+States
CISM Prep Course	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=9877&catid=191&country=United+States
CISSP Prep Course	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=8029&catid=191&country=United+States
Computer Hacking Forensic Investigator	EC-Council, Online, http://www.eccouncil.org/Course-Outline/CHF1%20Course.htm
Contingency Planning	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11919&catid=191&country=United+States
Cyber Law	EC-Council, Online, http://www.eccouncil.org/Course-Outline/CyberLaw%20Course.htm
Defending Windows Networks	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=10836&catid=191&country=United+States
DIACAP – Certification and Accreditation Process	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11776&catid=191&country=United+States
DIACAP – Certification and Accreditation Process, Executive Overview	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11778&catid=191&country=United+States
Disaster Recovery	EC-Council, Online, http://www.eccouncil.org/Course-Outline/Disaster%20Recovery%20Course.htm
E-Business Security	EC-Council, Online, http://www.eccouncil.org/Course-Outline/e-Security%20Course.htm
E-Commerce Architect	EC-Council, Online, http://www.eccouncil.org/Course-Outline/E-Commerce%20Architect%20Course.htm
ESCA/LPT	EC-Council, Online, http://www.eccouncil.org/Course-Outline/ECSA-LPT-Course.htm
Ethical Hacking and Countermeasures	EC-Council, Online, http://www.eccouncil.org/Course-Outline/Ethical%20Hacking%20and%20Countermeasures%20Course.htm



Foundstone Ultimate Hacking	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=978&catid=191&country=United+States
Foundstone Ultimate Hacking Expert	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=7938&catid=191&country=United+States
Foundstone Ultimate Web Hacking	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=979&catid=191&country=United+States
INFOSEC Certification and Accreditation Basics	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11905&catid=191&country=United+States
INFOSEC Forensics	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11943&catid=191&country=United+States
INFOSEC Strategic Planning	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11933&catid=191&country=United+States
Linux Security	EC-Council, Online, http://www.eccouncil.org/Course-Outline/Linux%20Security%20Course.htm
Mandiant Incident Response	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/wwwsearch.asp?country=United+States&keyword=9806
Network Management	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11937&catid=191&country=United+States
Network Security Administrator (ENSA)	EC-Council, Online, http://www.eccouncil.org/Course-Outline/ENSA.htm
Network Vulnerability Assessment Tools	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11784&catid=191&country=United+States
NIST 800-37 - Security Certification and Accreditation of Federal Information Systems	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11780&catid=191&country=United+States
NIST 800-37 - Security Certification and Accreditation of Federal Information Systems - Executive Overview	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11782&catid=191&country=United+States
Policy and Procedure Development	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11923&catid=191&country=United+States
Project Management in IT Security	EC-Council, Online, http://www.eccouncil.org/Course-Outline/Project%20Management%20in%20IT%20Security%20Course%20Outline/Project%20Management%20in%20IT%20Security%20Course%20Outline.html
Red Hat Enterprise Security: Network Services	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=7972&catid=191&country=United+States

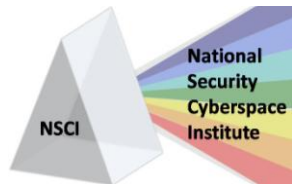


Risk Analysis and Management	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11913&catid=191&country=United+States
Security Certified Network Architect	Security Certified Program, Self-Study, http://www.securitycertified.net/getdoc/ac8d836b-cb21-4a87-8a34-4837e69900c6/SCNA.aspx
Security Certified Network Professional	Security Certified Program, Self-Study, http://www.securitycertified.net/getdoc/6e1aea03-2b53-487e-bab6-86e3321cb5bc/SNCP.aspx
Security Certified Network Specialist	Security Certified Program, Self-Study, http://www.securitycertified.net/getdoc/f6d07ac4-abc2-4306-a541-19f050f32683/SCNS.aspx
Security for Non-security Professionals	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=8461&catid=191&country=United+States
SSCP Prep Course	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=9876&catid=191&country=United+States
Vulnerability Management	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11941&catid=191&country=United+States

CYBER BUSINESS DEVELOPMENT OPPORTUNITIES

Note: Dates and events change often. Please visit web site for details. Please provide additions, updates, and/or suggestions for the CYBER calendar of events [here](#).

Office	Title	Link
DLA Acquisition Locations	Information Technology (IT) Information Assurance Support and Management Services, Defense Distribution Center (DDC)	https://www.fbo.gov/spg/DLA/J3/DDC/SP3300-09-R-0046/listing.html
Procurement Directorate	DoD DMZ Engineering Support	https://www.fbo.gov/spg/DISA/D4AD/DITCO/RFICBest/listing.html
Procurement Directorate	Mission Assurance and NetOps Support Services	https://www.fbo.gov/index?s=opportunity&mode=form&id=f991db8d4fbe6c91f4c14f5ceac6f492&tab=core&_cvview=1
Procurement Directorate	DISA Implementation of Web Audit Log Collection and Analysis Tools	https://www.fbo.gov/spg/DISA/D4AD/DITCO/DISAWEBAUDIT/listing.html
Procurement Directorate	Domain Name System (DNS) Security Support	https://www.fbo.gov/spg/DISA/D4AD/DITCO/DomainNameSystemDNS/listing.html
Procurement Directorate	Combined Federated Battle Lab Network (CFBLNet) Support	https://www.fbo.gov/spg/DISA/D4AD/DTN/RFI-CFBLNet/listing.html
PEO STRICOM	D--Threat Computer Network Operation (CNO) Teams for Test and Evaluation events	https://www.fbo.gov/index?s=opportunity&mode=form&id=d713ee539a271238c8580dd6042731ea&tab=core&_cvview=0



Department of the Air Force	A+, Network+, Security+ Training and Certification	https://www.fbo.gov/spg/USAF/ACC/99CONS/F3G3FA9167AC02/listing.html
Department of the Air Force	D -- AIR FORCE SYSTEMS NETWORK	https://www.fbo.gov/spg/USAF/AFMC/ESC/R2249/listing.html
Department of the Air Force	Cyberspace Infrastructure Planning System (CIPS)	https://www.fbo.gov/notices/1b8c4a285fa49e45f64aa7c997a69107
Air Force Materiel Command	Integrated Cyber Defense & Support Technologies	https://www.fbo.gov/index?s=opportunity&mode=form&id=cd045a392c920683ccb0b03df09bb134&tab=core&_cview=1
Air Force Materiel Command	D -- NETCENTS-2 NETOPS AND INFRASTRUCTURE SOLUTIONS (SMALL BUSINESS COMPANION)	https://www.fbo.gov/index?s=opportunity&mode=form&id=97c0d60d40e512c427dcb15ecf6daf5d&tab=core&_cview=1
Air Force Materiel Command	D -- NETCENTS-2 NETOPS AND INFRASTRUCTURE SOLUTIONS	https://www.fbo.gov/spg/USAF/AFMC/ESC/FA8771-09-R-0018/listing.html
Air Force Materiel Command	R -- NETCENTS-2 ENTERPRISE INTEGRATION SERVICE MANAGEMENT	https://www.fbo.gov/index?s=opportunity&mode=form&id=c570097dc6ed6b7f21476eadb2de55a9&tab=core&_cview=1
Air Force Materiel Command	R -- NETCENTS-2: IT PROFESSIONAL SUPPORT/ENGINEERING SERVICES	https://www.fbo.gov/index?s=opportunity&mode=form&id=14eea73232f5349381807ac6d9dadb1&tab=core&_cview=1
Air Force Materiel Command	Cyber Command and Control (C2) Technologies	https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA0809-RIKA/listing.html
Air Force Materiel Command	USAF Electronic Warfare Battle Management Technology CRFI	https://www.fbo.gov/spg/USAF/AFMC/ASC/USAF_Electronic_Warfare_Battle_Management_Technology/listing.html
Air Force Materiel Command	CompTIA Security+ Training	https://www.fbo.gov/spg/USAF/AFMC/88CONS/FA8601-09-T-0049/listing.html
Air Force Materiel Command	Military Communications and Surveillance Technologies and Techniques	https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA-09-09-RIKA/listing.html
Air Force Materiel Command	CyberSoft VFind Security Tool Kit Maintenance & Support	https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/FA8751-09-Q-0379/listing.html
Air Force Materiel Command	Provide Information Awareness (IA) training	https://www.fbo.gov/spg/USAF/AFMC/75/F2DC/CR9180A001/listing.html
Air Force Materiel Command	D – NETCENTS-2 Netops and Infrastructure Solutions	https://www.fbo.gov/spg/USAF/AFMC/ESC/FA8771-09-R-0018/listing.html
Air Force Materiel Command	D – NETCENTS-2 NETOPS and Infrastructure Solutions (Small Business Companion)	https://www.fbo.gov/spg/USAF/AFMC/ESC/FA8771-09-R-0019/listing.html
Air Force Materiel Command	Security Certificate & Accreditation Services for Information Systems	https://www.fbo.gov/spg/USAF/AFMC/75/FA8201-09-R-0088/listing.html



Air Force Materiel Command	A -- National Intelligence Community Enterprise Cyber Assurance Program (NICECAP)	https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/Reference-Number-BAA-06-11-IFKA/listing.html
Air Combat Command	A+, Network+, Security+ Training and Certification	https://www.fbo.gov/spg/USAF/ACC/99CONS/F3G3FA9167AC02/listing.html
Air Mobility Command	IA Certification & Accreditation Process	https://www.fbo.gov/spg/USAF/AMC/HQAMCC/EVSC1000/listing.html
Army Contracting Command	D--Information Assurance (IA) certification examinations	https://www.fbo.gov/notices/0c51687d4892095ccfed35a6f691dafe
United States Marine Corps	R--Internet Monitoring Services	https://www.fbo.gov/spg/DON/USMC/M67004/M6700409T0108/listing.html
Bureau of Industry & Security	International Competitive Bidding (ICB): Implementation and Support of NATO Enterprise	https://www.fbo.gov/spg/DOC/BIS/comp99/IFB-CO-12870-NEDS/listing.html
Department of the Army	D--Information Assurance, Engineering System Solutions Development, Testing, Deployment and Life Cycle Support	https://www.fbo.gov/spg/USA/DABL/DABL01/W91QUZ-09-0000/listing.html
Business Transformation Agency	Sources sought or request for information (RFI), DoD Information Assurance (IA) Controls (For Information Purposes Only)	https://www.fbo.gov/spg/ODA/BTA/BTA-BMD/HQ0566-09-InformationAssurance/listing.html
National Aeronautics and Space Administration	U--CISSP CERTIFICATION EDUCATION	https://www.fbo.gov/spg/NASA/GRC/OPDC2020/NNC09306220Q/listing.html
Washington Headquarters Services	BAA - Research and Studies for the Office of Net Assessment (OSD/NA)	https://www.fbo.gov/spg/ODA/WHS/WHSAPO/HQ0034-ONA-09-BAA-0002(1)/listing.html
Defense Advanced Research Projects Agency	Cyber Genome Program Proposers' Day	https://www.fbo.gov/index?s=opportunity&mode=form&id=0eff97ec44aada63117f050bc43d86f&tab=core&cvview=0



EMPLOYMENT OPPORTUNITIES WITH NSCI

<u>Job Title</u>	<u>Location</u>
Operational Deterrence Analyst	NE, VA
Defensive Cyber Ops Analyst	NE, VA, CO
Cyber SME	NE, VA, TX, CO
Geospatial Analyst	NE
Logistics All-Source Intelligence Analyst	NE
SIGINT Analyst	NE, CO
Cyber Operations SME	NE
Website Maintainer	NE
Cyberspace Specialists	NE
Cyberspace Manning IPT	NE

CYBERPRO CONTENT / DISTRIBUTION

<p>Officers</p> <p>President Larry K. McKee, Jr.</p> <p>Chief Operations Officer Jim Ed Crouch</p> <p>-----</p> <p>CyberPro Editor-in-Chief Lindsay Trimble</p> <p>CyberPro Research Analyst Kathryn Stephens</p> <p>CyberPro Archive</p>	<p>The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest and to keep subscribers who are involved in the development of Cyber-related concepts and initiatives informed on items of common interest. The newsletter and the information contained therein are not intended to provide a competitive advantage for any commercial firm. Any misuse or unauthorized use of the newsletter and its contents will result in removal from the distribution list and/or possible administrative, civil, and/or criminal action.</p> <p>The views, opinions, and/or findings and recommendations contained in this summary are those of the authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or National Security Cyberspace Institute.</p>
<p>To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.</p> <p>Please contact Lindsay Trimble regarding CyberPro subscription, sponsorship, and/or advertisement.</p>	

All rights reserved. CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.