



CyberPro

Volume 2, Edition 26
December 31, 2009

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 CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.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..... 5

Cyberspace – Big Picture..... 6

 Compliance will come of age in 2010 6

 Security warnings – and safety tips – for 2010..... 6

 Hot security predictions for 2010 6

 4 out-of-the-norm cybersecurity challenges 6

 Quentin Hardy on the Internet 7

Cyberspace – U.S. Government..... 7

 Prioritizing U.S. cybersecurity 7

 For Tom Talleur, cybersecurity is a bad situation about to get worse 8

 NIST ready to take on new cybersecurity tasks 8

 As attacks increase, U.S. struggles to recruit computer security experts 8

 Commerce Department gets funds to combat cyber espionage 8

 Feds need to push forward on cybersecurity, says former FBI CIO..... 9

 Congressional cybersecurity training to focus on awareness 9

 Acting cybersecurity ‘czar’ speaks out..... 9

 Who should be in charge of cybersecurity?..... 9

U.S. Cyber Czar Announced..... 10

 Finally, a cyber czar 10

 President Barack Obama identifies five priority areas for the new cybersecurity coordinator Howard Schmidt, as he is greeted with a positive response..... 10

 On deck: The cyber deputy..... 10

 Add workforce woes to cybersecurity chief’s agenda..... 10

 Capitol Hill: Wait and see on cybersecurity coordinator 11

 Melissa Hathaway’s advice to Howard Schmidt 11

 Schmidt: A take-no-nonsense cybersecurity ‘czar’ 11

 Obama cyber czar pick looks to secure smartphones, social nets..... 11

 National cybersecurity coordinator choice widely applauded 12

Cyberspace – Department of Defense (DoD) 13

 Pentagon reviewing strategic information operations..... 13

 Q&A: David Wennergren, DoD Deputy CIO 13



Encryption of Predator video feeds will take time.....	13
Report: Drone feeds gave insurgents ‘early warning’	13
Predator drones use less encryption than your TV, DVDs	13
Navy CIO Carey blogs about measuring cybersecurity	14
Report: Programmer conned CIA, Pentagon into buying bogus anti-terror code.....	14
Cyberspace – Department of Homeland Security (DHS)	15
DHS, Michigan launch cybersecurity partnership EINSTEIN-ONE	15
Cyberspace – International	15
Should the U.S. destroy jihadist Web sites?.....	15
IDF bolstering computer defenses.....	16
How cyberwarfare has made MI a combat arm of the IDF	16
Chinese hackers linked to ‘Warmergate’ climate change leaked e-mails controversy.....	16
China to create ‘white list’ of approved Web sites	16
Chinese ISP hosts 1 in 7 Conficker infections	16
U.S.-China Internet forum highlights need to step up online security	17
North Korea’s cyberspying streak.....	18
Military investigates hacking of Seoul’s war operations plan	18
Hackers may have accessed defense plans	18
Global spam king fined in Australia	18
Blighty to get own ‘cyber range’	18
Cyberspace Research	19
Cybercriminals will target filesharing sites in 2010, warn security experts.....	19
File sharing networks top target for cyber criminals	19
Conficker jams up developing interwebs	19
26C3: Network design weaknesses	19
Researcher demonstrates mobile phone weakness.....	20
Adobe to become top hacker target for 2010	20
Microsoft IIS vuln leaves users open to remote attack	20
Cyberspace Hacks and Attacks	21
The 9 coolest hacks of 2009.....	21
Report: FBI probes hacker attack on Citigroup	21
FBI probes hack at Citibank.....	21
Citigroup, law enforcement refute cyber heist report.....	21



CyberPro

Volume 2, Edition 26
December 31, 2009

Keeping Cyberspace Professionals Informed

Microsoft doesn't rule out rushed patch for IIS zero-day vulnerability.....	21
Anti-COFEE tool DECAF revealed as spoof	22
Amazon hit by DDoS attack.....	22
Hacker breaks Kindle's proprietary e-book protection.....	22
Hackers break Amazon's Kindle DRM	23
How the Koobface worm gang makes money	23
Hackers take Twitter offline for a while	23
Iranian hacker attack: What will it cost Twitter?.....	23
The bright side of \$26 drone hacks	23
SkyGrabber is for porn, not for hacking predator drones	24
Facebook hit by clickjacking attack	24
Cyberspace Tactics and Defense	25
Fixing the security disconnect.....	25
Good guys bring down the Mega-D botnet.....	25
Cyberspace - Legal	26
Why can't the law get the crooks?.....	26
TJX hacker mulls Asperger's defense	26
Home Secretary unmoved by last-ditch McKinnon protests.....	26
Cyberspace-Related Conferences	27
Cyberspace-Related Training Courses	29
Cyber Business Development Opportunities	31
Employment Opportunities with NSCI.....	34
CyberPro Content/Distribution	34



THIS WEEK IN CYBERPRO

BY LINDSAY TRIMBLE, NATIONAL SECURITY CYBERSPACE INSTITUTE, INC.

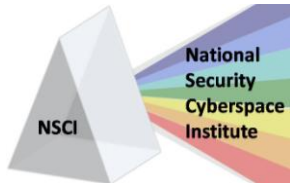
After a year of anticipation, U.S. President Barack Obama announced the appointment of Howard Schmidt as the first national cybersecurity czar. Many believe Schmidt's role as the cybersecurity adviser during the Bush administration and his positions with eBay and Microsoft have prepared him for the challenge ([page 10](#)). As cybersecurity czar, Schmidt will report to the National Security Council and the National Economic Council.

Obama has identified five key areas for Schmidt to focus on: developing a comprehensive strategy for protecting American networks; developing a unified response plan for future cyber incidents; strengthening public/private partnerships and international partnerships; promoting research and development of new technologies; and leading a campaign to promote cyber education and awareness ([page 10](#)). A *Federal Computer Week* article states it will also be important for Schmidt to close the "technical skill gap" and work with the federal government to improve recruitment, hiring and training for cyber professionals ([page 10](#)).

Schmidt has said he also hopes to encourage cyber education and research, stressing that cybersecurity is as important as physical security ([page 11](#)). Information technology professionals are enthusiastic about Schmidt's appointment ([page 12](#)). Alan Paller, director of research at the SANS Institute, said Schmidt has "demonstrated that he can forge sufficient support to overcome resistance and get things done" ([page 11](#)). The next step will be to name a deputy cyber coordinator. Sources report that Sameer Bhalotra is the leading candidate ([page 10](#)).

Many security predictions have been made for 2010. Nick Garlick, managing director for Nebulas Solutions Group, says compliance will be a critical part for organizations and cloud computing will show "drastic growth" next year ([page 6](#)). Don Gray, chief security strategist for Solutionary, predicts that social networking sites will experience significant breaches and better security procedures will be needed in healthcare ([page 6](#)). *Network World's* Andreas Antonopoulos reports that security funding will increase by at least 10 percent in 2010, mobile phones will be a new target for hackers and we'll see new regulatory compliance mandates from Congress ([page 6](#)).

The entire [NSCI](#) team wishes you a Happy New Year and a prosperous 2010!



CYBERSPACE – BIG PICTURE

Compliance will come of age in 2010

SECURITY PARK
12/30/2009

Nick Garlick, managing director for Nebulas Solutions Group, discusses the “IT Security Landscape” for 2010. Garlick says compliance will begin to be a critical part of organizations, with the introduction of new standards and implementation of best practices. He adds that firewall technology will improve and large vendors will acquire specialists for their skills and knowledge. Finally, 2010 will see “drastic growth” in cloud computing, although few companies will move to a “public cloud” model.
http://www.securitypark.co.uk/security_article_264093.html

Security warnings – and safety tips – for 2010

BY: JON SWARTZ, USA TODAY
12/21/2009

Don Gray, chief security strategist for Solutionary, discusses his security predictions for 2010. Gray says social networking sites will suffer significant breaches that could drive away users, and that healthcare reform will lead to a need for better healthcare security procedures. Gray adds that the National Breach Disclosure Law will help to protect consumers and that cloud computing will complicate business security.
<http://content.usatoday.com/communities/technologylive/post/2009/12/security-warnings---and-safety-tips---for-2010/1>

Hot security predictions for 2010

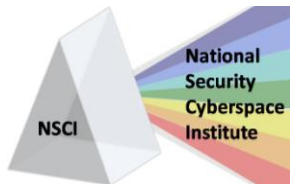
BY: ANDREAS M. ANTONOPOULOS, NETWORK WORLD
12/16/2009

Author Andreas Antonopoulos shares security predictions for 2010. The article says security funding will increase by at least 10 percent and that Congress will likely release new regulatory compliance mandates. Mobile phones will be a target for hackers and cloud computing providers will likely introduce encryption-at-rest and other security capabilities as a service. Antonopoulos believes the FBI will issue tens of thousands of security letters in order to get records on individuals without warrants, and that Real ID will be left behind in 2010.
<http://www.networkworld.com/columnists/2009/12/1609antonopoulos.html>

4 out-of-the-norm cybersecurity challenges

BY: ERIC CHABROW, GOVINFOSECURITY.COM
12/24/2009

During a panel presentation at a Federal CIO Council conference, Navy CIO Robert Carey discusses top IT security challenges. Carey said getting “non-tech decision makers” to understand cybersecurity is an important challenge, as well as speeding up development and investment to match the pace of the Internet’s growth. He added that identity management and determining who has what responsibilities in an organization is often difficult, and that wireless devices must be made more secure.
<http://blogs.govinfosecurity.com/posts.php?postID=396>



Keeping Cyberspace Professionals Informed

Quentin Hardy on the Internet

FORBES

12/22/2009

Quentin Hardy, national editor of *Forbes Magazine*, shares predictions about the future of technology in areas such as the Internet, print media, social networking sites and others. Overall, he believes that "at some point soon something really big will happen – a monster

virus, a terrorist hack, theft on an inordinate scale – that will call the whole thing into question."

<http://www.forbes.com/2009/12/08/internet-google-microsoft-technology-sneak-peek-10-hardy.html>

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 – U.S. GOVERNMENT

Prioritizing U.S. cybersecurity

BY: GREG BRUNO, COUNCIL ON FOREIGN RELATIONS
12/28/2009

In this article, Council on Foreign Relations' Greg Bruno interviews James Lewis, director of the Technology and Public Policy Program for the Center for Strategic and International Studies. Lewis discusses recent reports which found that militants in Iraq and Afghanistan were able to intercept live Predator drone feeds

from the U.S. military. Lewis says this is not surprising and that the U.S. has known about the vulnerabilities in these feeds since Bosnia. He also recommends that the downlinks between the drones and the ground be encrypted to better protect the information. Lewis discusses how President Barack Obama has addressed cybersecurity in 2009 and answers questions about the "international treaty on cyberwarfare" that has been the focus



of recent talks between Russia and the United States.

http://www.cfr.org/publication/21052/prioritizing_us_cybersecurity.html

For Tom Talleur, cybersecurity is a bad situation about to get worse

BY: JILL R. AITORO, NEXTGOV.COM
12/23/2009

In this article, Nextgov senior reporter Jill Aitoro interviews forensic technologist Tom Talleur, who has worked as a federal criminal investigator with NASA and the Defense Department. Talleur answers questions about threats to federal agencies and improvements to cybersecurity since President Barack Obama took office. Talleur also discusses the challenges to catching cyber criminals. Talleur says there is too much information to investigate everything, and that there aren't enough resources yet for investigating cyber crimes.

http://www.nextgov.com/nextgov/ng_20091223_7195.php

NIST ready to take on new cybersecurity tasks

BY: ERIC CHABROW, GOVINFOSECURITY.COM
12/24/2009

This article discusses new legislation that would give the National Institute of Standards and Technology more responsibility in developing cybersecurity standards. In an interview with GovInfoSecurity.com, new NIST Director Patrick Gallagher says he is ready to accept new responsibilities and discusses creating an NIST computer security laboratory and the potential reorganization of NIST. Gallagher also answers questions about funding needed and the specific reorganization plans proposed by NIST Information Technology Laboratory Director Cita Furlani.

http://www.govinfosecurity.com/articles.php?art_id=2029

As attacks increase, U.S. struggles to recruit computer security experts

BY: ELLEN NAKASHIMA AND BRIAN KREBS,
WASHINGTON POST
12/23/2009

This article discusses how the federal government is struggling to recruit skilled computer-security workers, and says a bidding war has begun between agencies and contractors because there are so few skilled technicians with security clearances. The Pentagon is reporting difficulties with staffing their new Cyber Command. National security experts worry that the lack of trained professionals to defend federal networks "is leading to serious gaps in protection and significant losses of intelligence." The article discusses how the shortage of skilled professionals is leading to increases in salaries and "job-hopping."

<http://www.washingtonpost.com/wp-dyn/content/article/2009/12/22/AR2009122203789.html>

Commerce Department gets funds to combat cyber espionage

BY: JILL R. AITORO, NEXTGOV.COM
12/21/2009

The 2010 Consolidated Appropriations Act, signed into law Dec. 16 by President Barack Obama, includes more than \$100 million for Commerce's Bureau of Industry and Security, and includes \$10 million for an initiative to combat cyber espionage. The \$10 million will fund an increase in cybersecurity personnel and security enhancements to computer systems that maintain sensitive data about international trade, including illegal export activities.

http://www.nextgov.com/nextgov/ng_20091221_5373.php?oref=topnews



Feds need to push forward on cybersecurity, says former FBI CIO

BY: J. NICHOLAS HOOVER, INFORMATION WEEK
12/23/2009

The Federal Bureau of Investigation's former CIO, Zal Azmi, says the government needs to "develop and implement a comprehensive cybersecurity plan." Azmi is currently the senior VP for government contractor CACI's cyber solutions group. President Barack Obama recently appointed Howard Schmidt to be the White House cybersecurity coordinator, and has "tasked him with creating a comprehensive cybersecurity strategy." Azmi says any effective plan must focus on hardware, software and people, and must view cybersecurity as "a risk management effort." Azmi also recommends encouraging public-private partnerships and finding ways to bring innovative cybersecurity products into the government.

<http://www.darkreading.com/security/government/showArticle.jhtml?articleID=222100083>

Congressional cybersecurity training to focus on awareness

FEDERAL NEWS RADIO
12/16/2009

Congressional staff will now undergo new cybersecurity training. House leaders have requested a new training regimen for aides and additional measures to protect sensitive information. Employees that travel outside of the United States will also be required to have their government-issued wireless devices checked by security before and after trips.

<http://www.federalnewsradio.com/?nid=15&sid=1841720>

Acting cybersecurity 'czar' speaks out

GOVINFOSECURITY.COM
12/15/2009

After nearly seven months since President Barack Obama said he would name a permanent cybersecurity coordinator to report to the White House national security and national economic advisors, the job remains vacant. Chris Painter, White House acting senior director for cybersecurity, says the Obama administration isn't missing a step in tackling key information security challenges, even without the position. Painter did not address when a permanent White House cybersecurity coordinator would be appointed, but said "It's a mistake to think that without a coordinator we're not making progress."

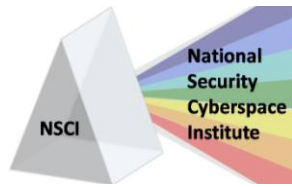
http://www.govinfosecurity.com/articles.php?art_id=2008

Who should be in charge of cybersecurity?

BY: LARRY SELTZER, PC MAG
12/21/2009

The National Cyber Advisor, promised by President Barack Obama during the presidential campaign, remains an element of unfinished business as 2009 comes to an end. The proposed Cybersecurity Coordinator position is not what the campaign promised and reportedly has a long list of candidates who have turned the position down.

http://blogs.pcmag.com/securitywatch/2009/12/who_should_be_in_charge_of_cyb.php



U.S. CYBER CZAR ANNOUNCED

Finally, a cyber czar

BY: ANDY GREENBERG, FORBES
12/21/2009

President Barack Obama recently announced that Howard Schmidt would be the nation's first cybersecurity coordinator. Schmidt has extensive experience in cybersecurity, including previous positions in the government and in large corporations such as eBay and Microsoft. Schmidt will report to the National Security Council and the National Economic Council.
<http://www.forbes.com/2009/12/21/cyber-czar-named-security-business-in-the-beltway-schmidt.html>

President Barack Obama identifies five priority areas for the new cybersecurity coordinator Howard Schmidt, as he is greeted with a positive response

BY: DAN RAYWOOD, SC MAGAZINE
12/23/2009

In a video address, Howard Schmidt says there are five areas that President Barack Obama has identified for him to focus on as the cybersecurity coordinator to the White House: developing a comprehensive strategy for protecting American networks; developing a unified response plan for future cyber incidents; strengthening public/private partnerships as well as international partnerships; promoting research and development of new technologies; and leading a campaign to promote cyber education and awareness. The selection of Schmidt for the position has received positive response from several cybersecurity experts.
<http://www.scmagazineuk.com/president-barack-obama-identifies-five-priority-areas-for-the-new-cybersecurity-coordinator-howard-schmidt-as-he-is-greeted-with-a-positive-response/article/160219/>

On deck: The cyber deputy

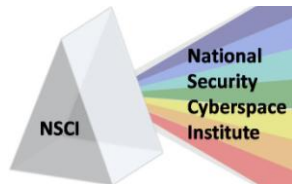
BY: GAUTHAM NAGESH, NEXTGOV.COM
12/23/2009

After a long wait, President Barack Obama has announced the appointment of Howard Schmidt as the nation's first cybersecurity czar. Some say the next step could be a deputy cyber coordinator, possibly from the Senate Select Committee on Intelligence. Sources say Sameer Bhalotra is the leading candidate for the position. Bhalotra has worked with the CIA in the science and technology directorate and was a member of the Commission on Cybersecurity for the 44th Presidency.
http://techinsider.nextgov.com/2009/12/cyber_deputy_coming_soon.php

Add workforce woes to cybersecurity chief's agenda

BY: MAX STIER, FEDERAL COMPUTER WEEK
12/24/2009

This article discusses how the new White House cybersecurity coordinator, Howard Schmidt, must address the "shortage of highly skilled cybersecurity professionals in government." While there is a need for effective cyber policies, better software and better information technology management, it will be very important for Schmidt to look at "closing the technical skill gap" which will allow the federal government to better recruit, hire and train cybersecurity professionals. There are currently no government certification standards or a federal career path for cybersecurity specialists and federal scholarship programs are "inadequately funded."
<http://fcw.com/articles/2009/12/24/max-stier-howard-schmidt-cybersecurity-workforce.aspx>



Capitol Hill: Wait and see on cybersecurity coordinator

BY: MAX CACAS, FEDERAL NEWS RADIO
12/23/2009

Senator Joe Lieberman (D-Conn.) recently spoke to Federal News Radio and said he will introduce legislation that requires the Senate to confirm the new White House cybersecurity coordinator. Lieberman added that even though Senate confirmation is not required, he will invite Howard Schmidt to testify to the Homeland Security Committee to hear his ideas for improving cybersecurity. Rep. Jim Langevin from Rhode Island said he is glad that President Barack Obama has finally appointed a cybersecurity coordinator, but that there is a lot of work to be done now. Langevin also says he would like to know the extent of authority that will be given to Schmidt.

<http://www.federalnewsradio.com/?nid=35&sid=1848067>

Melissa Hathaway's advice to Howard Schmidt

BY: ERIC CHABROW, GOVINFOSECURITY.COM
12/23/2009

Melissa Hathaway, former White House acting senior director of cyberspace, offers advice for the new White House cybersecurity coordinator, Howard Schmidt. Hathaway says the initial challenges for Schmidt will be building relationships, communication, transparency and learning the core missions and capabilities of all of the different departments and agencies. Hathaway says Schmidt will then have to review the progress that has been made against the top 25 recommendations in the Cyberspace Policy Review; learn the critical path programs of the Comprehensive National Cybersecurity Initiative (CNCI); assist departments and agencies in advocating for fiscal 2011 funding; and understand the legislative landscape.

<http://blogs.govinfosecurity.com/posts.php?postID=394>

Schmidt: A take-no-nonsense cybersecurity 'czar'

BY: ERIC CHABROW, GOVINFOSECURITY.COM
12/22/2009

Alan Paller, director of research at the SANS Institute, says President Barack Obama's choice for cybersecurity coordinator – Howard Schmidt – will “surprise a lot of people in Washington” and that he “has demonstrated that he can forge sufficient support to overcome resistance and get things done.” In a video on the White House Web site, Schmidt said he will focus on the following areas: developing a comprehensive cybersecurity strategy; security U.S. critical information networks; creating a unified response plan for cyber incidents; strengthening public-private and international partnerships; and promoting research and development of new technologies.

http://www.govinfosecurity.com/articles.php?article_id=2022

Obama cyber czar pick looks to secure smartphones, social nets

BY: TIM GREENE, COMPUTERWORLD
12/22/2009

The article discusses how the new U.S. cybersecurity coordinator, Howard Schmidt, hopes to encourage education and research that will help to develop more secure products for users. Schmidt said cybersecurity should be considered as important as physical security and that smartphones and mobile devices generate the most concern. He added that vendors and purveyors of social media sites need to better educate their users about threats, and that IT workers should consent to background checks. Schmidt also discusses cloud computing and how we can make strong authentication the rule instead of the exception.

http://www.computerworld.com/s/article/9142595/Obama_cyber_czar_pick_looks_to_secure_smartphones_social_nets?taxonomyId=17



National cybersecurity coordinator choice widely applauded

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS

12/22/2009

Many in the information technology industry have applauded President Barack Obama's decision to appoint Howard Schmidt as the first cybersecurity coordinator. Roger Thornton, chief technology officer of Fortify Software, says Schmidt is a perfect choice because of his extensive experience in the government with

the Defense Department, as well as in industry. Schmidt was the cybersecurity adviser during the Bush administration, and was also chief information security officer at both Microsoft and eBay. Alan Paller, director of research at the Sans Institute, says Schmidt was an appropriate choice given the challenges that the job entails.

<http://gcn.com/articles/2009/12/22/cybersecurity-coordinator-schmidt-reaction.aspx>

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



- 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





CYBERSPACE – DEPARTMENT OF DEFENSE (DoD)

Pentagon reviewing strategic information operations

BY: WALTER PINCUS, WASHINGTON POST
12/27/2009

Defense Secretary Robert Gates has several studies underway to “get a firmer grip over the individual military services’ plans for strategic communications next year.” Gates is attempting to determine what the specific role of the Defense Department is in federal cybersecurity. The White House recently decided to “hold biweekly interagency meetings to coordinate activities of the Defense and State departments.”

<http://www.washingtonpost.com/wp-dyn/content/article/2009/12/26/AR2009122601462.html>

Q&A: David Wennergren, DoD Deputy CIO

BY: J. NICHOLAS HOOVER, INFORMATION WEEK
12/23/2009

Department of Defense deputy CIO David Wennergren was interviewed by Information Week and answered questions about the military’s SOA strategy and how the definition of net-centricity is changing. Wennergren explained how the military is using cloud computing and how he keeps track of the military’s massive IT budget. Finally, he answered questions about procurement reform, and what will change because of the new U.S. Cyber Command.

<http://www.informationweek.com/news/government/leadership/showArticle.jhtml?articleID=222002806>

Encryption of Predator video feeds will take time

BY: WILLIAM WELSH, FEDERAL COMPUTER WEEK
12/21/2009

Ellen Nakashima from the *Washington Post* reports it could take as many as five years

before video feeds from Predator drones can be fully encrypted. U.S. forces recently discovered that insurgents were able to intercept video footage from the unmanned aerial vehicles. According to the Air Force Unmanned Aircraft Systems Flight Plan, the Air Force has begun encrypting the UAV fleet, but that the work will not be completed until 2014.

<http://fcw.com/articles/2009/12/21/predator-video-feed-encryption.aspx>

Report: Drone feeds gave insurgents ‘early warning’

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
12/21/2009

An anonymous Air Force official tells the *Air Force Times* that a militant group in Iraq was able to stay ahead of U.S. forces after intercepting transmissions from spy drones, despite Pentagon reports that militants have not been able to make a dent in U.S. operations. U.S. forces found footage shot by Predator drones and smaller unmanned aerial vehicles on laptops confiscated during a raid in Baghdad. Col. Gregory Gonzalez explains that drone feeds are easy to intercept because they broadcast their feeds unencrypted and in every direction.

<http://www.wired.com/dangerroom/2009/12/drone-feeds-gave-insurgents-early-warning-report/>

Predator drones use less encryption than your TV, DVDs

BY: NATE ANDERSON, ARSTECHNICA
12/17/2009

This article discusses how no encryption was used to send transmissions between the Predator drones and ground control, allowing Iraqi insurgents to intercept the feeds. The U.S. government has reportedly known about this flaw since the U.S. campaign in Bosnia in the



1990s, but the Pentagon assumed local adversaries would not know how to exploit it. The military is looking into encrypting the downlink between the drone and ground control, but experts warn that retrofitting is hard and off-the-shelf encryption tools don't all work on the Predator.

<http://arstechnica.com/tech-policy/news/2009/12/predator-drones-use-less-encryption-than-your-tv.ars>

Navy CIO Carey blogs about measuring cybersecurity

FEDERAL NEWS RADIO
12/21/2009

Rob Carey, chief information officer at the Department of the Navy, discusses how to measure cybersecurity in a recent blog post. Carey said metrics could help measure performance but that defining these IT metrics has proved challenging. He also discusses how malicious programs are spreading through hyperlinks and how social networking or real-time search sites are being exploited.

<http://www.federalnewsradio.com/?nid=19&sid=1846392>

Report: Programmer conned CIA, Pentagon into buying bogus anti-terror code

BY: KIM ZETTER, WIRED BLOG NETWORK
12/28/2009

Programmer Dennis Montgomery, who claims he has produced software to detect hidden terrorist messages in Al Jazeera broadcasts, is also "apparently responsible for a false alert in 2003 that grounded international flights." Montgomery faked software demonstrations and tricked the Pentagon into investing in his program that may never have existed. This article discusses how Montgomery has tricked the government into investing in his programs in the past, by claiming that he found hidden messages in barcodes in terrorist videos and by receiving a contract from the Air Force to handle video shot by unmanned Predator drones. Montgomery reportedly received \$2 million from the Air Force as recently as last February.

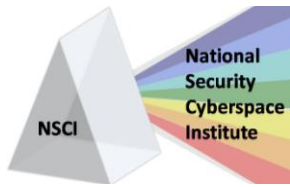
<http://www.wired.com/threatlevel/2009/12/montgomery-2>



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 – DEPARTMENT OF HOMELAND SECURITY (DHS)

DHS, Michigan launch cybersecurity partnership EINSTEIN-ONE

FEDERAL NEWS RADIO
12/15/2009

The Department of Homeland Security recently announced its new partnership with the state of Michigan to deploy the federally-developed cybersecurity technology EINSTEIN-ONE to

Michigan's cyber networks. The EINSTEIN-ONE technology helps analysts spot malicious activity that can threaten government network systems.

<http://www.federalnewsradio.com/index.php?nid=19&sid=1841168>

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

CYBERSPACE – INTERNATIONAL

Should the U.S. destroy jihadist Web sites?

BY: MARK THOMPSON, TIME.COM
12/23/2009

This article discusses how jihadist recruiters are using the Internet to find new recruits – often without any face-to-face contact at all. A recent

report from MEMRI, the Middle East Media Research Institute, has said that disabling just a few key jihadist domains could “cripple Islamists’ ability to conduct online mass discussions” and “hamper the rapid spread of jihad material.” Still, some experts warn that

110 Royal Aberdeen • Smithfield, VA 23430 • ph. (757) 871-3578



simply disabling extremist Web sites will not completely cripple jihadist efforts. Evan Kohlmann of the NEFA Foundation, also points out that shutting down these domains would hurt us, since we gather valuable information from the sites. Some experts argue that we should participate on these forums, arguing with young Muslims over what the Koran actually allows.

<http://www.time.com/time/nation/article/0,8599,1949373,00.html>

IDF bolstering computer defenses

BY: YAAKOV KATZ, THE JERUSALEM POST
12/17/2009

The Israeli Defense Force is responding to growing cyber warfare threats by enhancing its defenses against enemy hackers. "The threat is always growing and we always need to be one step ahead," a senior IDF officer said Wednesday. "There are attempts all the time to try and hack into our networks, and we are aware of our enemies' capabilities."

<http://www.jpost.com/servlet/Satellite?cid=1260930892360&pagename=JPost%2FJPArticle%2FShowFull>

How cyberwarfare has made MI a combat arm of the IDF

BY: ANSHEL PFEFFER, REUTERS
12/17/2009

Israeli Military Intelligence chief Maj. Gen. Amos Yadlin says using computer networks for espionage is as important today as the advent of air support was to warfare in the 20th century. Yadlin says cyber espionage gives small countries, terror groups and even individuals the power to launch cyber attacks. Experts are calling for more coordination between agencies.

<http://www.haaretz.com/hasen/pages/1135422.html>

Chinese hackers linked to 'Warmergate' climate change leaked e-mails controversy

BY: JASON LEWIS AND SIMON PARRY,
DAILYMAIL.CO.UK
12/27/2009

The Mail has traced the messages stolen from the University of East Anglia's climate change department back to a suspect computer that provides Internet access to China. The stolen messages "cast doubt on the reliability of scientists' global warming claims" and were originally posted by a computer company in Siberia. Chinese hackers are often behind cyber attacks, since the Chinese government supports the hackers. *The Mail* has traced the stolen e-mails to the "so-called Open Access server run by Malaysian telecoms giant Telekom Malaysia Berhad."

<http://www.dailymail.co.uk/news/worldnews/article-1238638/Chinese-hackers-linked-Warmergate-climate-change-leaked-emails-controversy.html#ixzz0augDnCV0>

China to create 'white list' of approved Web sites

BY: GREG PALKOT, FOX NEWS
12/22/2009

In a country that has an estimated 350 million Web users, the Chinese government has demanded that all Web sites register their domain names with the government. Sites such as Twitter, YouTube and Facebook are already blocked by Beijing in an effort to restrict Internet access and the availability of alternate information for its citizens.

<http://www.foxnews.com/scitech/2009/12/22/china-create-white-list-approved-web-sites/>

Chinese ISP hosts 1 in 7 Conficker infections

BY: ROBERT MCMILLAN, COMPUTERWORLD
12/17/2009

According to data released this week by Shadowserver, China Telecom's Chinanet seems



Keeping Cyberspace Professionals Informed

to have had a harder time battling the Conficker worm than have other ISP's. The virus began spreading late last year and received much attention earlier in the year, including a late March segment on "60 Minutes," warning of an April 1 upgrade to the worm.

http://www.computerworld.com/s/article/9142414/Chinese_ISP_hosts_1_in_7_Conficker_infections

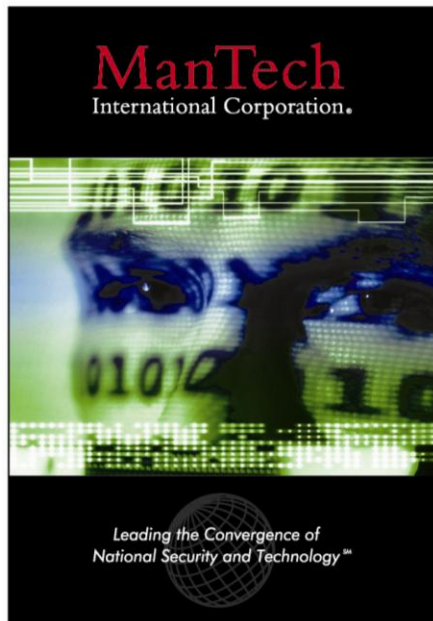
U.S.-China Internet forum highlights need to step up online security

CHINAVIEW.CN
12/11/2009

The third annual U.S.-China Internet Industry Forum in San Francisco, Calif., concluded with delegates calling for more efforts to step up online security. The U.S.-China Internet

Industry Forum was launched in 2007 and has been held previously in Seattle, Wash., and Shanghai, China. "If network information security is not guaranteed, the information flow will become irregular. If illegal and harmful information are allowed to flow rampantly without checks, it will do great harm to the real society," said Cai Mingzhao, former deputy director of China's State Council Information Office and an adviser to the Internet Society of China. Robert Hormats, undersecretary from the U.S. Department of State, agreed and believes the United States and China should strengthen cooperation to jointly address network security risks.

http://news.xinhuanet.com/english/2009-12/11/content_12631544.htm



ManTech's Cyber Solution Center Helps Combat Threats to our National Infrastructure

ManTech International Corporation is a leading provider of innovative technologies and solutions for mission-critical national security programs for the Intelligence Community; the departments of Defense, State, Homeland Security and Justice; the Space Community and other U.S. federal government customers. It has recently established a Cyber Solution Center that marshals expertise from across the company to help the U.S. government and private industry fight the increasing threats to our IT and communications infrastructure. ManTech has been providing cyber operations services to the U.S. government and private industry for 11 years and its cyber security professionals 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. For additional information on ManTech's Cyber Solutions contact Mark Root at: mark.root@ManTech.com



North Korea's cyberspying streak

BY: ANDY GREENBERG, FORBES
12/21/2009

North Korean hackers reportedly intercepted confidential South Korean defense strategy plans in November, after a South Korean military officer left a USB key plugged into his PC while accessing the public Internet. The stolen documents are said to have contained detailed information about possible U.S. and South Korean pre-emptive strikes against North Korea. Jim Lewis, Center for Strategic and International Studies, says North Korea has developed a cyber espionage program that sets North Korea above most other countries in terms of international espionage competence. <http://www.forbes.com/2009/12/21/korea-hackers-software-technology-cio-network-hackers.html>

Military investigates hacking of Seoul's war operations plan

BY: SONG SANG-HO, KOREA HERALD
12/19/2009

Military authorities are investigating a recent hack in which criminals stole classified educational material on Korea-U.S. combined war plan "OPLAN 5027." The material was leaked in November when a military officer at the Combined Forces Command connected his USB drive to an unsecured computer. Authorities report that other material on the USB drive was leaked, but that it was not confidential information. Authorities believe the hacker is part of the North Korean cyber warfare unit. http://www.koreaherald.co.kr/NEWKHSITE/data/html_dir/2009/12/19/200912190012.asp

Hackers may have accessed defense plans

DEFENSE NEWS
12/18/2009

Computer hackers believed to be from North Korea have reportedly gained access to a

confidential U.S.-South Korean defense plan. The hackers used a Chinese IP address to access military data related to the defense plan, called Operation Plan 5027. A spokesman from the South Korean Defense Ministry said an investigation is underway to determine how much the leakage will affect South Korean military plans.

<http://www.defensenews.com/story.php?i=4425624>

Global spam king fined in Australia

ENTERPRISE SECURITY TODAY
12/23/2009

Lance Atkinson of New Zealand was recently fined by an Australian court for his part in a syndicate that was able to send 10 billion spam messages per day. Atkinson was fined for breaching the Spam Act 2003. The syndicate reportedly had operations in the United States, Australia, New Zealand, China, India, Russia and Canada, and accounts for up to one-third of the world's junk e-mails. The syndicate was originally found by British journalist Simon Cox, who traced spam e-mails that he received back to Shane Atkinson in New Zealand.

http://www.enterprise-security-today.com/story.xhtml?story_id=70742

Blighty to get own 'cyber range'

BY: LEWIS PAGE, THE REGISTER
12/18/2009

The United Kingdom recently announced it is working on a "cyber range" – a "simulated network world where weapons-grade government malware and countermeasures can be tried out." The project is part of the UK programme called SATURN (Self-organising Adaptive Technology under Resilient Networks), but will include involvement from U.S. firm Northrop Grumman.

http://www.theregister.co.uk/2009/12/18/uk_cyber_range/



CYBERSPACE RESEARCH

Cybercriminals will target filesharing sites in 2010, warn security experts

BY: CLAUDINE BEAUMONT, TELEGRAPH.CO.UK
12/29/2009

Computer experts at Kaspersky Labs predict hackers will increasingly launch attacks through filesharing networks. Alex Gostev, the director of global research and analysis team at Kaspersky, says industry will be forced to develop more complex protection tools to combat more sophisticated attacks in 2010. Experts also warn that mobile phones are “of interest to cybercriminals” and could face increased threats in 2010. Kaspersky Labs said fake antivirus scams would likely decrease in 2010 because of the growth of the fake antivirus market and falling profits for cybercriminals.

<http://www.telegraph.co.uk/technology/news/6872622/Cybercriminals-will-target-filesharing-sites-in-2010-warn-security-experts.html>

File sharing networks top target for cyber criminals

BY: ANURADHA SHUKLA, TECHWORLD
12/18/2009

Security Company Kaspersky Lab anticipates some changes in cyber criminal activity in the new year and has outlined the threats it expects to see. According to Kaspersky, cyber criminals have changed their strategy and, in 2010, they will no longer attack via Web sites and applications, but will be more focused on attacking computers through file sharing networks.

<http://news.techworld.com/security/3208976/file-sharing-networks-top-target-for-cyber-criminals>

Conficker jams up developing interwebs

BY: JOHN LEYDEN, THE REGISTER
12/17/2009

New research from Shadowserver says the Conficker worm has “disproportionally affected computer systems in the developing world” and that “developing nations have become malware ghettos.” Security experts believe the Conficker authors were more successful in infecting PCs than they thought they would be, and that they have held off on doing anything with the botnet in efforts to attract the least amount of attention.

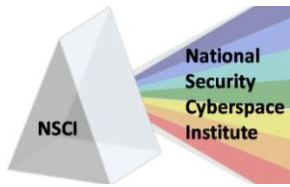
<http://www.theregister.co.uk/2009/12/17/conficker/>

26C3: Network design weaknesses

BY: STEFAN KERMPPL, THE H SECURITY
12/29/2009

At the 26th Chaos Communication Congress (26C3) conference in Berlin, security researcher Fabian Yamaguchi presented several vulnerabilities that are “found in many average communication networks and affect all layers from the access layer to the application layer.” These minor design flaws can be combined to allow hackers to launch dangerous attacks. This article discusses how Yamaguchi demonstrated the vulnerabilities across several layers. Yamaguchi warned his audience that no vulnerability is isolated, and that “the security of network components depends on that of their respective environments.”

<http://www.h-online.com/security/news/item/26C3-Network-design-weaknesses-893356.html>



Researcher demonstrates mobile phone weakness

BY: ROBERT MCMILLAN, TECHWORLD
12/29/2009

Researcher Karsten Nohl presented at the Chaos Communication Conference in Berlin, and demonstrated weaknesses in GSM phone security. GSM-cracking tools are already available to law enforcement, and Nohl believes that criminals could be using the tools as well to listen in on mobile phone calls. Nohl explains that the vulnerability is caused by the 20-year-old encryption algorithm used by most carriers, which "is simply too weak." The GSM Alliance reports that GSM phones make up about 80 percent of the mobile market. A spokeswoman with the GSM Association says they are looking into the researcher's claim, and that they have developed a next-generation standard called A5/3 which is much more secure.

<http://news.techworld.com/security/3209282/researcher-demonstrates-mobile-phone-weakness>

Adobe to become top hacker target for 2010

BY: PHIL MUNCASTER, V3.CO.UK
12/29/2009

The 2010 Threat Predictions report from McAfee warns users and information security

professionals that the biggest increase in threats for 2010 will affect social networks, and that Adobe products will replace Microsoft for the No. 1 software target for cyber criminals. The report identified Flash and Acrobat Reader as the favorite vector among attackers because they are so widely distributed. The report also said attacks will increase on social networks as user numbers continue to grow.

<http://www.v3.co.uk/v3/news/2255480/adob-become-top-hacker-target>

Microsoft IIS vuln leaves users open to remote attack

BY: DAN GOODIN, THE REGISTER
12/25/2009

Researcher Soroush Dalili recently identified a vulnerability in Microsoft's Internet Information Services, caused by the way that IIS parses file names with colons or semicolons in them, allowing hackers to run malicious code on victims' machines. Some researchers, such as vulnerability tracker Secunia, classified the bug as "less critical," although Dalili rated the vulnerability "highly critical." Microsoft says they are investigating the report, and that they have not yet seen any attacks that target the vulnerability.

http://www.theregister.co.uk/2009/12/25/microsoft_iis_semicolon_bug/



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 HACKS AND ATTACKS

The 9 coolest hacks of 2009

BY: KELLY JACKSON HIGGINS, DARK READING
12/23/2009

In this article, *Dark Reading* looks at the nine most profound hacks of 2009. The article details hacks including hijacking application updates, the Bill Gates 'LinkedIN' Invite, ATM malware and the browser-based darknet.

http://www.darkreading.com/vulnerability_management/security/attacks/showArticle.jhtml?articleID=222003008

Report: FBI probes hacker attack on Citigroup

MSNBC
12/22/2009

According to reports by the *Wall Street Journal*, the FBI is investigating a hacker attack on Citigroup, Inc. that led to the theft of millions of dollars. The article reported that the attack on Citigroup's Citibank subsidiary was detected over the summer and that the FBI, the National Security Agency, the Homeland Security Department and Citigroup worked together to investigate the attack. Joe Petro, managing director of Citigroup's Security and Investigative services, denies the report.

http://www.msnbc.msn.com/id/34521131/ns/business-us_business/

FBI probes hack at Citibank

BY: SIOBHAN GORMAN AND EVAN PEREZ, WALL STREET JOURNAL
12/22/2009

This article claims that the Federal Bureau of Investigation is looking into a security breach targeting Citigroup Inc. that resulted in the loss of tens of millions of dollars and may be linked to a Russian cyber gang. Joe Petro, managing director of Citigroup's Security and Investigative services, says there was no breach of their system and no losses to customers or the bank.

http://online.wsj.com/article/SB126145280820801177.html?mod=googlenews_wsj

Citigroup, law enforcement refute cyber heist report

BY: JEREMY KIRK AND ROBERT MCMILLAN,
COMPUTERWORLD
12/22/2009

Citigroup and a federal law enforcement source are refuting a *Wall Street Journal* report that claimed Citigroup customers had lost millions of dollars in a cyber heist over the summer. The report said the FBI is investigating the theft, and that hackers used malicious software created in Russia to steal the money. A federal law enforcement source called the article "inaccurate" and says the reports "confused a known 2007 hack of Citigroup-branded automated teller machines with a long-running criminal effort to hack online banking customers and move money out of their accounts." Citigroup says there has been no breach of their systems, and that there have been no customer or bank losses.

http://www.computerworld.com/s/article/9142619/Citigroup_law_enforcement_refute_cyber_heist_report

Microsoft doesn't rule out rushed patch for IIS zero-day vulnerability

BY: ROBERT WESTERVELT, SEARCHSECURITY.COM
12/28/2009

Microsoft recently acknowledged a zero-day vulnerability in their Internet Information Services (IIS) that could allow attackers to upload malicious code on a Web server. A report from Canada-based security firm IPSS Inc. shows how the exploit code works on IIS 6 and prior versions. Microsoft security program manager Jerry Bryant says the vulnerability is not highly critical and that Microsoft has not



seen an attack so far that exploits the vulnerability.

http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1377741,00.html

Anti-COFFEE tool DECAF revealed as spoof

BY: NICK EATON, SEATTLE PI BLOGS
12/18/2009

Two developers claimed they had created a tool, called DECAF, that kills Microsoft's COFFEE computer-forensics tool, but experts claim the tool was only a publicity stunt. The developers say they staged the stunt to "raise awareness for security and the need for better forensic tools." The DECAF Web site says that "governments should not rely on a tool to automate the process of forensics but rather invest in the education of investigators and forensic tool experts."

<http://blog.seattlepi.com/microsoft/archives/188706.asp>

Amazon hit by DDoS attack

BY: PETER SAYER, TECHWORLD
12/24/2009

DNS provider, UltraDNS, was recently the target of a DDoS attack that prevented Internet users in parts of California from reaching several sites, including Amazon. Amazon Web Services (AWS) was the first to report the incident, and workers at Neustar – the owner of UltraDNS – were able to analyze the attack pattern and take steps to

limit its effects. Allen Goldberg, vice president of corporate communications at Neustar, says the attack was limited to Northern California users, and that they were able to contain the attack in "well under an hour."

<http://news.techworld.com/security/3209224/amazon-hit-by-ddos-attack>

Hacker breaks Kindle's proprietary e-book protection

BY: PATRICIA RESENDE, ENTERPRISE SECURITY TODAY
12/23/2009

Hackers were recently able to crack Kindle's copyright protection, which could force Amazon to follow the lead of Apple in offering DRM-free content. An Israeli hacker, who goes by Labba, says he can break the Kindle's digital-rights management protection, which allows electronic books to be viewed on non-Kindle devices. The hacker reportedly asked for help in his hack on an Israeli Web site, hacking.org. Amazon has not yet responded to the hack, but is expected to release a patch and update for the Kindle device. Some experts believe Amazon may follow Apple's lead and offer DRM-free content rather than patching the flaw only to be hacked again.

http://www.enterprise-security-today.com/story.xhtml?story_id=70778

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.



Hackers break Amazon's Kindle DRM

BY: DAN GOODIN, THE REGISTER
12/23/2009

U.S. and Israeli hackers say they have found a way to break copyright protections built into Amazon's Kindle for PC. Amazon representatives have not yet responded to the demonstration. The hackers released software, called unswindle, which uses reverse engineering to crack the encryption algorithm used by the Mobipocket reader and most Kindle books. Once the software is installed, most Amazon ebooks can be converted to the Mobi format.

http://www.theregister.co.uk/2009/12/23/amazon_kindle_hacked/

How the Koobface worm gang makes money

BY: KELLY JACKSON HIGGINS, DARK READING
12/21/2009

New research released from Trend Micro says Koobface's creators make money mostly through scareware or fake antivirus, click fraud, information-stealing malware and online dating services. David Perry, global director of education for Trend Micro, says Koobface is "an ongoing criminal enterprise using hundreds and thousands of pieces of code." The Koobface group has been linked to five different fake antivirus groups and the worm is able to install a variant of the Ldpinch information-stealing Trojan that can steal user credentials and either resell them or use them to hack Web sites.

http://www.darkreading.com/vulnerability_management/security/attacks/showArticle.jhtml?articleID=222002862

Hackers take Twitter offline for a while

BY: SUMNER LEMON, COMPUTERWORLD
12/18/2009

Hackers who call themselves the Iranian Cyber Army were able to take Twitter offline last week by changing DNS records and redirecting users

to another Web page. Visitors to Twitter were taken to a page that showed a green flag and Arabic writing, with the heading "this site has been hacked by the Iranian Cyber Army." Twitter blamed the attack on changes made to the company's DNS records, and says the company's servers were never compromised. http://www.computerworld.com/s/article/9142458/Hackers_take_Twitter_offline_for_a_while

Iranian hacker attack: What will it cost Twitter?

BY: LAURENT BELSIE, THE CHRISTIAN SCIENCE MONITOR
12/18/2009

The recent attack against the popular Twitter microblogging service was a "sophisticated online blitz – perhaps part of an online Iranian cybercampaign – that could prove costly for social media networks." Ron Deibert, a cyberwarfare researcher at the University of Toronto, says several nations have developed operational doctrines in cyberspace, and that "in such a climate of intense militarization," attacks like the ones against Twitter will become more common. The Twitter hackers redirected users to a page that showed a picture of a flag with Farsi script, and said "this site has been hacked by Iranian Cyber Army." The article discusses how an attack like this can damage Twitter's reputation and future profitability.

<http://www.csmonitor.com/Money/2009/1218/Iranian-hacker-attack-What-will-it-cost-Twitter>

The bright side of \$26 drone hacks

BY: SPENCER ACKERMAN, THE WASHINGTON INDEPENDENT
12/22/2009

Naval blogger Galrahn recently discussed the *Wall Street Journal* story which said Iraqi insurgents used an off-the-shelf \$26 hack to intercept feeds from U.S. unmanned aerial vehicles. Galrahn says the short-term solution to the issue is not to encrypt the data, but



rather to use the unencrypted video stream to go after the insurgents by including packet data in the stream that exploits software vulnerabilities.

<http://washingtonindependent.com/71694/the-bright-side-of-26-drone-hacks>

SkyGrabber is for porn, not for hacking predator drones

BY: ROBERT GRAHAM, DARK READING
12/18/2009

Recent news stories claim Iraqi insurgents were able to intercept live feeds from Predator drones with the \$26 off-the-shelf software product, SkyGrabber. This article explains that SkyGrabber is actually a packet sniffer, and could not eavesdrop on the drone feeds. The software is most popular because it is able to download free porn, but the software does not allow the user to watch videos in real-time, making it impossible to use the program to watch a live video feed. In order to intercept the Predator feeds, hackers would need a product that is compatible with the Predator, although these tools do exist and may come off-the-shelf.

http://www.darkreading.com/blog/archives/2009/12/predator_vs_sky.html

Facebook hit by clickjacking attack

BY: KELLY JACKSON HIGGINS, DARK READING
12/23/2009

Facebook recently experienced a clickjacking attack, where an attacker hides a malicious link or malware on a legitimate Web site that appears to be normal content. In the attack on Facebook, the malicious link appeared to be a comment on a user's account which requested that the victim click on a photo. The victim was taken to a YouTube video and the post was left on the victim's account to infect his or her friends. Facebook has since blocked the URL to the malicious site and is cleaning up accounts where the link was posted. Robert Hansen, CEO of SecTheory, says clickjacking attacks will likely increase on social networking sites, and warns users to be cautious when clicking any suspicious posts or links.

<http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=222100098>

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.



CYBERSPACE TACTICS AND DEFENSE

Fixing the security disconnect

BY: JOHN SAWYER, DARK READING
12/24/2009

Author John Sawyer discusses the “disconnect” between “network groups, system administrators, developers and similar groups.” He says security teams are often seen as the bad guys because they must block access to sites or because their work is inconvenient to users. Sawyer also discusses how “best practices call for least privilege” and the balance between security and functionality or productivity.

http://www.darkreading.com/blog/archives/2009/12/closing_the_sec.html;jsessionid=3DPCLF WIZHW3PQE1GHPCKH4ATMY32JVN

Good guys bring down the Mega-D botnet

BY: ERIK LARKIN, PC WORLD
12/27/2009

FireEye researcher Atif Mushtaq has been helping defend clients’ networks from the

Mega-D botnet for the past two years, and was recently able to take down the botnet after studying how the botnet was operated. The group from FireEye contacted domain-name registrars that hold records for the domain names Mega-D used for its control servers, as well as ISPs that hosted the command-and-control servers. FireEye picked up the spare domain names Mega-D’s controllers listed in the programming and pointed them to sinkholes to track the botnet. Joe Stewart, director of malware research with SecureWorks, says FireEye had “a major victory” but questions the long-term impact of the takedown.

<http://www.networkworld.com/news/2009/12/2809-good-guys-bring-down-the.html?hpg1=bn>



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



CYBERSPACE - LEGAL

Why can't the law get the crooks?

BY: LINCOLN SPECTOR, PC WORLD
12/26/2009

This article explains that, even when authorities are able to catch cybercriminals, there are "20 more waiting to take their place." Cybercrimes are highly profitable and any criminal with an Internet connection can launch attacks. Punishments are also fairly light, and it is still very difficult to identify criminals. Technology lawyer Mark Grossman says the methods that are needed to catch cybercriminals require too much time and resources and may require international cooperation.

<http://www.networkworld.com/news/2009/12/2609-why-cant-the-law-get.html?hpg1=bn>

TJX hacker mulls Asperger's defense

BY: DAN GOODIN, THE REGISTER
12/16/2009

Attorneys for Albert Gonzalez, the international hacker who has admitted to stealing 130 million payment card numbers, are saying Gonzalez suffers from Asperger's syndrome – postponing the hacker's hearing. Gonzalez has provided

"extensive information" to the government, including names of people he worked with. Gonzalez also drew prosecutors a map that helped them find more than \$1.1 million he had buried.

http://www.theregister.co.uk/2009/12/16/albert_gonzalez_aspergers/

Home Secretary unmoved by last-ditch McKinnon protests

BY: JOHN LEYDEN, THE REGISTER
12/16/2009

Despite recent protests, Home Secretary Alan Johnson told MPs Tuesday that self-confessed Pentagon hacker Gary McKinnon ought to answer serious criminal charges in the United States. Medical opinion revealed the autism sufferer is a suicide risk. Johnson's decision is the subject of the latest in a series of judicial review challenges by the McKinnon family and legal team and judges will now decide on whether or not to proceed with a full hearing.

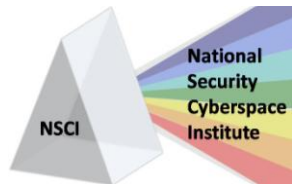
http://www.theregister.co.uk/2009/12/16/mckinnon_protest/



High Tech Problem Solvers

www.qtri.gatech.edu

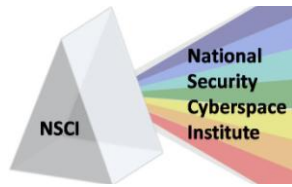
From accredited DoD enterprise systems to exploits for heterogeneous networks, GTRI is on the cutting edge of cyberspace technology. Transferring knowledge from research activities with the Georgia Tech Information Security Center, GTRI is able to bring together the best technologies, finding real-world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



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](#).

14 Jan 2010	Army IT Day 2010 , Vienna, VA; http://www.afceanova.org/events/special-events/it-days/army-it-day-fy10
20 – 22 Jan 2010	TechNet 2010 , Orlando, FL; http://www.afcea-orlando.org/?pg=events/TechNet2010/TechNet2010
22 – 29 Jan 2010	2010 DoD Cyber Crime Conference , St. Louis, Missouri; http://www.dodcybercrime.com/10CC/
27 Jan 2010	State of the Net Conference , Washington DC; http://www.netcaucus.org/conference/2010/
27 – 28 Jan 2010	Cyber Warfare 2010 , London, UK; http://www.cyberwarfare-event.com/Event.aspx?id=228104
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+Sponsorhips+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 – 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
26 – 28 Mar 2010	EuroForensics Conference , Istanbul, Turkey; http://euroforensics.com/



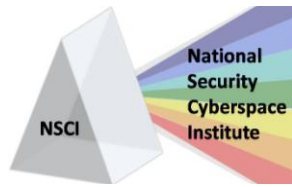
29 – 30 Mar 2010	Information Assurance – Latest Requirements and Methods , Washington, DC; http://www.ttcus.com/view-seminar.cfm?id=88
30 – 31 Mar 2010	AFCEA Belvoir Industry Days 2010 , National Harbor, MD; http://fbcinc.com/event.aspx?eventid=Q6UJ9A00L29J
07 – 08 April 2010	9th Annual Security Conference , 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
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
24 – 27 May 2010	CEIC , Las Vegas, NV; http://www.ceiconference.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/



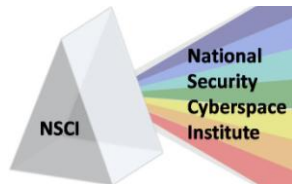
CYBERSPACE-RELATED TRAINING COURSES

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

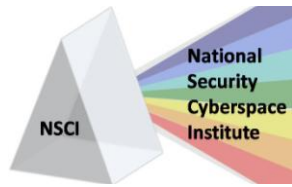


Risk Analysis and Management	Global Knowledge, Dates and Locations: http://www.globalknowledge.com/training/course.asp?pageid=9&courseid=11913&catid=191&country=United+States
Security Certified Network Architect	Security Certified Program, Self-Study, http://www.securitycertified.net/getdoc/ac8d836b-cb21-4a87-8a34-4837e69900c6/SCNA.aspx
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	A+, Network+, Security+ Training and	https://www.fbo.gov/spg/USAF/ACC/99CONS/F



the Air Force	Certification	3G3FA9167AC02/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	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
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



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.