## Officers

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>President</td>
<td>Larry K. McKee, Jr.</td>
</tr>
<tr>
<td>Chief Operations Officer</td>
<td>Jim Ed Crouch</td>
</tr>
<tr>
<td>CyberPro Editor-in-Chief</td>
<td>Lindsay Trimble</td>
</tr>
<tr>
<td>CyberPro Research Analyst</td>
<td>Kathryn Stephens</td>
</tr>
</tbody>
</table>

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.

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.

To subscribe or unsubscribe to this newsletter click here [CyberPro News Subscription](#).

Please contact Lindsay Trimble regarding CyberPro subscription, sponsorship, and/or advertisement.

---

**All rights reserved. CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.**
# Table of Contents

This Week in CyberPro................................................................. 5
Hacking: For good or evil?......................................................... 6
Cyberspace – Big Picture.......................................................... 8
  - Cyber Operations Span the Globe’s Largest Theater .................. 8
  - Panel: We Need Nationwide Broadband Internet Access ............. 8
  - U.S. Reinforces Importance of Security During Cyber Security Awareness Month .................................................. 8
  - Terrorists nearing ability to launch big cyberattacks against U.S. ........................................................................ 8
Cyberspace – U.S. Government................................................... 9
  - House to launch cybersecurity review ...................................... 9
  - Federal Taskforce To Focus On Cybersecurity Metrics ............... 10
  - New Security Paradigm Needed ............................................ 10
  - Critics warn ICANN agreement will cause Internet domain chaos ................................................................. 10
  - The Upside of Unbinding ICANN From U.S. Oversight ............. 10
  - Lawmakers and Industry Leaders Praise ICANN Deal ............... 10
  - U.S. ‘To Loosen’ Grip on Internet .......................................... 11
  - ICANN Seeks to Quell Concerns on the Hill ............................. 11
  - ICANN Freed From U.S. Gov’t Oversight ............................... 11
  - Is the Smart Grid Really Going to Happen? ............................ 11
U.S. Cyber Leadership Debate................................................. 12
  - The Real Cyber Czar ................................................................ 12
  - Federal Cyber Security: Still No Answer .................................. 13
  - DHS official says cyber czar ‘bad idea,’ cyber coordinator ‘great idea’ ................................................................. 13
  - Sen. Collins Says DHS Should Lead Cybersecurity, Not White House ................................................................... 13
Cyberspace – Department of Defense (DoD) .............................. 14
  - Cybersecurity vs. Cyber Warfare ........................................... 14
  - Cyber Defense – Lots Going On ............................................. 14
  - Collaborative Cyber Command ............................................. 14
  - U.S. Cyber Command Goes Online ....................................... 14
  - Military hackers could stop wars before they start .................. 15
  - Lynn Calls for Collaboration in Establishing Cyber Security ....... 15
  - Twitter is Mission Critical ..................................................... 15
Web 2.0 Review Could Lead to Restricted Use of Social Networking in DoD ................................................. 16
All eyes on DOD's social-media policies as review nears completion .......................................................... 16
Pentagon Web 2.0 Strategy Could Give Spies, Geeks New Roles ................................................................. 16
Defense to Allow Troops, Family Members to Use Social Network Sites .................................................... 16
DoD Preparing to Lift USB Ban ............................................................................................................... 17
Should the Marines set up a cyber command? ............................................................................................ 17
U.S. Navy creates command to maintain cyber supremacy .................................................................... 17

Cyberspace – Department of Homeland Security (DHS) ................................................................................. 18
U.S. urges 'cyber hygiene' effort. ................................................................................................................ 18
DHS Plans Cyber Job Fair ............................................................................................................................ 18
Homeland Security to hire up to 1K cyber experts .................................................................................. 18
Former DHS Cyber Czar Joins Wurldtech's Advisory Board ...................................................................... 18

Cyberspace – International .......................................................................................................................... 19
Singapore Beefs Up Cyber Security ........................................................................................................ 19
The Kremlin's Eeeevil New Plan to Rein in Bloggers ............................................................................. 19
Russian Cybergangs Make the Web A Dangerous Place ......................................................................... 19
Hackers Pay 43 Cents Per Hijacked Mac ................................................................................................. 19
U.K. already 'major world power' in cyberwar ....................................................................................... 20
New U.K. Cybersecurity Centre Opens Doors ......................................................................................... 20

Cyberspace Research .................................................................................................................................. 21
'State of the Internet' assessed .................................................................................................................. 21
Security Spending to Hit $14.5bm Says Gartner ......................................................................................... 21
U.S. broadband lags Asian nations .......................................................................................................... 21
Prototype security software blocks DDoS attacks ...................................................................................... 21
Researchers Hijack a Drive-By Botnet ...................................................................................................... 22
Economic espionage .................................................................................................................................. 22
Internet Has Never Been More Dangerous, Report Says ........................................................................ 23
Smart Grid Framework Vulnerable to Hackers – Report ...................................................................... 23
Research: Small DIY Botnets Prevalent in Enterprise Networks ............................................................ 23
Scareware and Bots Require Layered Defenses ....................................................................................... 24

Cyberspace Hacks and Attacks .................................................................................................................... 25
Cyber Gangs Hit Healthcare Providers .................................................................................................. 25
CyberPro

Keeping Cyberspace Professionals Informed

IRS Scam Now World’s Biggest E-Mail Virus Problem ........................................ 25
‘Money Mule’ Recruitment Network Exposed ..................................................... 25
Massive E-mail Phishing Attack Hits Web .......................................................... 25
Hackers and Scalper Pounce on Google Wave Invites ...................................... 26
Soldiers’ Data Still Being Downloaded Overseas, Firm Says ......................... 26
PandaLabs: Record-Breaking 5 Million New Threats In Third Quarter Of 2009 .... 26
Password-Stealing Malware Spikes ................................................................. 26
New Trojan Gives Criminals Full-Service Bank Theft ....................................... 27
Conficker Showdown: No End in Sight ............................................................. 27

Cyberspace Tactics and Defense ........................................................................ 28
Navigating the New Cybercrime Threatscape, Part 1 ......................................... 28
Navigating the New Cybercrime Threatscape, Part 2 ......................................... 28
Navigating the New Cybercrime Threatscape, Part 3 ......................................... 28
Battlefield High to host cyber security exercise ............................................... 28
Hacker Conference Starts Next Week ............................................................... 29
Microsoft Security Essentials Available for Download .................................... 29
The Difficulty of Un-Authentication .................................................................. 29
Sharing Threat Data is Key to Securing the Power Grid ................................... 29
Cyborgs for Cyber Defense .............................................................................. 30
Cyber Experts Learn from Ant Tactics .............................................................. 30
VeriSign Embeds Authentication Into Cisco SA 500 Series Security Appliances ... 30

Cyberspace - Legal ............................................................................................. 31
Lawmakers Weigh Government’s Role in Securing the Web ......................... 31
Senators Plan Bill to Advance Net Neutrality ............................................... 31
House Subcommittee Moves Bill to Boost Cybersecurity ............................ 31
Cybersecurity Bill Pushes University-Business Alliances ............................ 31
House Panel Approves Cyber-Security RandD Bill ....................................... 32
Panel Passes Cyber Workforce Reform .......................................................... 32

Cyberspace-Related Conferences ..................................................................... 33
Cyberspace-Related Training Courses ............................................................. 34
Cyber Business Development Opportunities ............................................... 37
Employment Opportunities with NSCI ............................................................ 39
CyberPro Content/Distribution ......................................................................... 39
**Keeping responsibility in cyber security is the focus of this year’s Cyber Security Awareness Month and reported data stresses the importance of being proactive. It has been projected that one in five citizens will be a victim of cyber crime in the future (page 8). To support Cyber Security Awareness Month this October, the Department of Homeland Security is encouraging all Internet users to perform “good hygiene,” including keeping security systems up-to-date and being wary of unknown senders in your e-mail’s in-box (page 18).**

The U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers (ICANN) signed a new agreement Sept. 30, allowing ICANN greater independence while giving more countries oversight of the organization (page 11). Critics fear that this agreement won’t require enough accountability from ICANN (page 10). Advocates, such as House Energy Commerce Chairman Henry Waxman and House Energy and Commerce Communications Subcommittee Chairman Rick Boucher say the agreement is an example of how a “public-private partnership can work to the advantage of all stakeholders” (page 10). Viviane Reding, the European Union’s commissioner for information society and media, believes ICANN’s new annual reports will allow ICANN to be more accountable to users around the world (page 11).

Department of Defense officials are discussing the differences between “cyber security” and “cyber warfare” – concluding that cyber warfare is more offensive (page 14). U.S. Deputy Defense Secretary William Lynn said recently that his department has faced threats from a variety of perpetrators – teenage hackers, organized criminals and foreign spies – at “astonishing speed” (page 15). One recommendation for defense against these threats is to hack enemy systems before they can enter cyber warfare. According to Naval Postgraduate School professor John Arquilla, this tactic will make enemies rethink entering a cyber war with the United States (page 15).

This edition includes summaries of a three-part series, called “Navigating the New Cybercrime Threatscape” (page 28). The three articles discuss cybercrime and cyber threats, highlighting cybercrime targets; malware, botnets and phishing; and strategies to protect your systems from cybercrime.

Cybercrime and the importance of taking cyber security into your own hands were both discussed at Hacker Halted USA 2009. I had the opportunity to attend this conference and provide some highlights from the three-day event in this week’s feature article (page 6).

Take advantage of this year’s Cyber Security Awareness Month by thinking about what you can do to make cyberspace more secure.
Hacking: For Good or Evil?

By Lindsay Trimble, National Security Cyberspace Institute, Inc.

In 2008, Miami was the headquarters for one of the largest criminal computer hacks of all time when Alberto Gonzalez managed a global operation to victimize major U.S. corporations. Just two weeks ago, Miami was the headquarters for hundreds of ethical hackers and information security professionals.

Hacker Halted USA 2009 was held in Miami from Sept. 23 to 25 and provided the opportunity for IT security experts, managers and industry leaders to interact about the current state of information security. This was the 14th Hacker Halted conference sponsored by the International Council of E-Commerce Consultants (EC-Council), an organization that certifies individuals in various e-business and security skills.

“Organizations worldwide are investing in infrastructure but lagging implementation, measurement and review of security and privacy policies,” wrote Jay Bavisi, EC-Council president, in his welcome letter. “But it is heartening to know that organizations are beginning to recognize that information security can deliver more than just protection for information. Information assets are critical to any business and paramount to the survival of any organization in today’s globalized digital economy.”

Some speakers discussed the more technical aspects of cyber security, including defense against malware and botnets; limitations in network security monitoring; and virtualization security. Exhibitors also highlighted next generation security software, information technology education and training solutions.

A common theme at the conference was the necessity to secure your part of cyberspace.

“You don’t save money by cutting security,” said Howard Schmidt, CEO of the Information Security Forum. In his talk, Schmidt listed steps that should be taken to secure your part of cyberspace. He said to get the basics right; don’t rely on historical data; plan for uncertainty; adapt to changes; and build for the future.

Ira Winkler, founder of the Internet Security Advisors Group and author of Zen and the Art of Information Security, also provided his ideas on improving cybersecurity.

“People don’t know what they don’t know about cybersecurity,” Winkler said, explaining that many cyber attacks exploit widely-known problems. Winkler echoed Schmidt in his promotion of learning the basics first.
“A ‘master’ understands the basics and sees simplicity in difficulty,” said Winkler. He stressed that “security is a must, not a ‘should.”’

A number of speakers focused on the intersection of crime and technology. In his talk “Jihad me this,” Treadstone 71’s Jeff Bardin discussed terrorist groups’ use of technology in recruitment and propaganda.

Jayson Street, Stratagem 1 Solutions, said that we need to “look at all of the facets of global cyber warfare to truly understand the problem.” He also predicted that warfare will be increasingly directed at a nation’s citizens to affect their perceptions, using the attacks on U.S. and South Korean government Web sites this year as an example.

Erik Laykin, Duffs & Phelps, examined the Gonzalez crime ring in detail and provided an overview of how the Internet is used in organized crime groups. In another talk, Bardin and Hugh Thompson, People Security, discussed the underground cyber economy. Thompson and Bardin addressed this serious topic in an entertaining way, providing an overview of the characters involved and the tactics used.

A highlight of the conference was EC-Council’s presentation of $1 million to the International Multilateral Partnership Against Cyber Threats (IMPACT). Headquartered in Malaysia, IMPACT is the first global public-private initiative against cyber terrorism. IMPACT works to ensure the protection and security of the 191 International Telecommunication Union member states’ cyberspaces and infrastructures.

Hacker Halted USA 2009 provided a prime example of the interaction in industry, government and academia that will be imperative for a secure cyberspace.
Cyberspace is being recognized as a potential warfare domain, which has implications for numerous nations and public and private entities. This idea is behind the AFCEA’s theme of “Cyber Operations: A Multinational Challenge” for its 24th annual TechNet Asia-Pacific conference and exposition in November. One problem in the use of cyber warfare is that countries can’t agree on whether such an act is considered an act of war, as was demonstrated with NATO discussions. If such lasting alliances can’t agree on the issue, Schneider writes, then it is unlikely such an agreement would be reached with Asian-Pacific nations since such alliances are much younger than NATO. The AFCEA’s November conference will focus “on the unique cyber issues in the Asia-Pacific region and what is being done to deal with them.”


Panel: We Need Nationwide Broadband

Internet Access
FROM: ASSOCIATED PRESS
10/02/2009

Internet access is important in being socially, economically and politically first class, said the president and CEO of the John S. and James L. Knight Foundation, which houses the Knight Commission on the Information Needs of Communities in a Democracy. After a two-year study, the commission found “that a free flow of information ‘is as vital to the healthy functioning of communities as clean air, safe streets, good schools and public health.’” In order to meet this vital element of society, Internet options should be increased and the government should ensure broadband and cable TV providers quickly enter the market of underserved areas with expansion incentives. The commission also addressed the problem of failing news corporations in the digital age.

http://www.foxnews.com/story/0,2933,559061 ,00.html

U.S. Reinforces Importance of Security During Cyber Security Awareness Month
BY: MARKETWIRE, YACHT CHARTERS MAGAZINE
10/01/2009

October became Cyber Security Awareness Month six years ago, and this year’s theme is focused on how all of society must work together to maintain cyber security. It has been projected that one in five citizens will become a victim of cyber crime. While drug trafficking used to be the No. 1 way of illegal moneymaking, cyber crime has now taken first place, according to Symantec. Internet security threats also increased last year, which should be a motivating factor in increasing awareness of cybersecurity.

http://www.yachtchartersmagazine.com/node/ 1127876#
Treaty to ensure cyberattack technology isn’t provided to terrorist organizations. He also said terrorist organizations could have cybercrime technology within a few years. A former CIA director said the organizations could use such technology to infiltrate power plants and bring down a country’s electrical grid.

http://www.nextgov.com/nextgov/ng_20091002_9081.php

---

**House to launch cybersecurity review**

**BY: CHRIS STROHM, CONGRESSIONAL DAILY**

10/01/2009

House Representative C.A. “Dutch” Ruppersberger (D-Md.) will hold a series of meetings with federal officials and private companies in hopes of producing a “comprehensive report with recommendations” on how to deal with and manage cybersecurity efforts in the United States. Ruppersberger serves as chairman to the House Intelligence Technical and Tactical Intelligence Subcommittee and on the House Appropriations Committee. Ruppersberger said he thinks President Barack Obama has unfortunately put cyber security “on the shelf” as other issues have been brought to the front of his agenda.

Federal Taskforce To Focus On Cybersecurity Metrics
BY: J. NICHOLAS HOOVER, INFORMATION WEEK
10/05/2009
The Security Metrics Taskforce has the job of coming up with a standard metric system that will be used to measure effectiveness of cybersecurity efforts throughout the government, said federal CIO Vivek Kundra. The taskforce “comes at a time where the Federal Information Security Management Act ... has been criticized for being inadequate and incomplete in terms of performance measurement,” according to this article. The taskforce will come up with a measurement system by looking at “best practices from federal agencies and the private sector.”

New Security Paradigm Needed
BY: JOEL N. GORDES AND MICHAEL MYLRE, HARTFORD BUSINESS
10/05/2009
A recent report from the CIA said cyber criminals have attacked “foreign power utilities with the goal of extorting money.” Thus Joel Gordes argues that the United States must develop cybersecurity, especially in terms of its energy infrastructure. One way to do this, he writes, would be to integrate security into the new “Smart Grid” design for the energy infrastructure.

Critics warn ICANN agreement will cause Internet domain chaos
BY: GRANT GROSS, TECHWORLD
10/02/2009
The new agreement between the Internet Corporation for Assigned Names and Numbers and the U.S. Department of Commerce, signed Sept. 30, has led to controversy among supporters and dissenters. Critics warn that the new agreement, which gives up the DOC’s control over ICANN and was conducted in secrecy, doesn’t require enough accountability within the organization. ICANN’s review panels will likely have the same politics as ICANN under the new agreement’s panel selection process, a critic of the agreement said. However, others disagree that the agreement was made in secrecy and that ICANN’s review panels will be biased toward ICANN’s politics and policies.

The Upside of Unbinding ICANN From U.S. Oversight
BY: TONY BRADLEY, PC WORLD
10/01/2009
Tony Bradley writes that it’s not a bad move for the United States to let ICANN, the Internet Corporation for Assigned Names and Numbers, become a global organization. Since the United States’ Department of Commerce has been against expanding the number of TLDs, Bradley thinks that the number of TLDs may now increase, which could simplify finding information on the Internet and free space on legitimate TLDs. However, the United States still has some power over the number of TLDs by maintaining control over the Internet Assigned Numbers Authority.

Lawmakers and Industry Leaders Praise ICANN Deal
BY: ANDREW NOYES, CONGRESSDAILY
09/30/2009
Lawmakers are praising the recent agreement that ensures a permanent relationship between the U.S. government and the Internet Corporation for Assigned Names and Numbers.
House Energy and Commerce Chairman Henry Waxman and House Energy and Commerce Communications Subcommittee Chairman Rick Boucher (D-Va.) say the agreement is an example of how “a public-private partnership can work to the advantage of all stakeholders.” ICANN has agreed to set up panels that will review areas such as network security; the evolution of domains; the continuance of a public database that includes Web site owners; and an accountability panel with a representative to the U.S. government.  

http://www.nextgov.com/nextgov/ng_20090930_4227.php

**U.S. ‘To Loosen’ Grip on Internet**  
BBC NEWS  
09/28/2009  
The U.S. government is expected to sign an “affirmation of commitments” with Internet regulator ICANN that will give the organization authority to run itself for the first time. ICANN was originally set up by the U.S. government, and is a not-for-profit, private sector corporation that oversees critical parts of the Internet, including the top-level domain name system. New rules about top level domains would allow companies to use brands as Web addresses and would include domain names in Asian, Arabic or other scripts. The report from ICANN also identified a number of groups, including representatives from foreign governments, which would review ICANN’s work.  

http://news.bbc.co.uk/2/hi/technology/8275679.stm

**ICANN Freed From U.S. Gov’t Oversight**  
BY: GRANT GROSS, NETWORK WORLD  
09/30/2009  
The Internet Corporation for Assigned Names and Numbers (ICANN) has reached a new agreement, called an Affirmation of Commitments, which allows the nonprofit more independence, while giving more countries oversight of the organization. The new agreement will require a review of ICANN’s performance every three years and recognizes ICANN as a “global private-sector led organization.” Viviane Reding, the European Union’s commissioner for information society and media, says that the new agreement will allow ICANN to be more open and accountable to users worldwide. ICANN will now publish annual reports that show the organization’s progress and will be more “transparent and accountable.”  


**ICANN Seeks to Quell Concerns on the Hill**  
BY: ANDREW NOYES, CONGRESSDAILY  
09/23/2009  
ICANN recently released a letter that says that the organization would maintain a “long-term, formal relationship with the U.S. government,” although the agreement between the ICANN and the National Telecommunications and Information Administration expires at the end of September. Rod Beckstrom, ICANN CEO, says that the organization is working to establish guidelines that state they will remain a U.S.-based nonprofit. Many industry stakeholders have criticized ICANN for seeking more independence from federal oversight, although others feel that no one entity should control the Internet’s infrastructure.  

http://www.nextgov.com/nextgov/ng_20090930_4227.php

**Is the Smart Grid Really Going to Happen?**  
BY: AMY MORRIS, FEDERAL NEWS RADIO  
09/24/2009  
Annabelle Lee, the senior cyber security strategist at the National Institute of Standards and Technology, says that the promises of a Smart Grid are “happening now” through “smart meter deployment.” George Arnold,
national coordinator for Smart Grid Interoperability at NIST, says that economics will drive the creation of the Smart Grid especially if consumers begin to better understand the benefits of the smart grid in terms of saving money, reducing usage and benefiting the environment. Arnold also says that there is a “sense of urgency behind the Smart Grid project” since so many parts of the Smart Grid are already being put into place without any standards from NIST.

http://www.federalnewsradio.com/?nid=255&sid=1770238

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

U.S. CYBER LEADERSHIP DEBATE

The Real Cyber Czar
BY: SHANE HARRIS, NATIONAL JOURNAL
10/05/2009
Though President Barack Obama has yet to appoint someone to become the nation’s cybersecurity official, departments and agencies within the government are working together to secure the nation’s cyberspace assets. National Security Agency Director Lt. Gen. Keith B. Alexander is already doing what the “cyber czar” would be working on, but unlike the unfilled cyber czar position, Alexander has a budget and authority. “In terms of actually doing the job [of cyber czar], it’s clear that the president already has someone — Alexander,” according to the article. The NSA will be working with the Department of Homeland Security to ensure the safety of public and private networks, said DHS Secretary Janet Napolitano, by providing “technical assistance” to DHS.

http://www.nextgov.com/nextgov/ng_20091005_2168.php
Federal Cyber Security: Still No Answer
BY: JON OLTSIK, CBS NEWS
09/22/2009
During the presidential campaign, President Barack Obama had promised to “make cyber security a priority in his administration” and “appoint a coordinator to oversee federal cyber security programs as soon as possible,” but the position still remains unfilled. This article discusses some of the most pressing items on the agenda for the new cyber security coordinator, including emergency response; training the public; developing a National ID program; pushing through FISMA 2.0; developing a better system for recruiting and keeping cyber security personnel; addressing Federal data privacy standards; addressing security compliance incentives in the private sector; unifying cyber security communications; and becoming a cyber security leader for the United States and a representative to other nations.

DHS official says cyber czar ‘bad idea,’ cyber coordinator ‘great idea’
BY: ANDREW NOYES, CONGRESSDAILY
10/02/2009
Homeland Security Deputy Undersecretary Philip Reitinger said that the extended process of choosing an official to lead the nation’s cybersecurity efforts hasn’t been a bad thing. “We need the right person, not just a person immediately,” Reitinger said. Reitinger said the official should be a “cyber coordinator” rather than a “cyber czar.” The legality of czars and their history will be discussed at a hearing planned by the Senate Judiciary Constitution Subcommittee chairman. Frank Kramer is considered to be the frontrunner for the cyber coordinator position, according to sources.
http://www.nextgov.com/nextgov/ng_20091002_4965.php

Sen. Collins Says DHS Should Lead Cybersecurity, Not White House
BY: CHRIS STROHM, CONGRESSDAILY
09/25/2009
Sen. Susan Collins (R-Maine), the Senate Homeland Security and Governmental Affairs ranking member, is preparing to introduce legislation that would make the Department of Homeland Security the primary authority in protecting federal civilian and private computer networks, rather than a cybersecurity czar from the White House. Collins says that the federal government needs to clarify who is in charge of cybersecurity and make sure that the officials and agencies are given the authority that they will need. Collins also says that her bill will “counter the Rockefeller-Snowe” bill because it would codify and strengthen cybersecurity responsibilities in the Homeland Security Department. If the legislation passes, the Defense Department and National Security Agency would be responsible for protecting defense networks.
http://www.nextgov.com/nextgov/ng_20090925_9014.php
Cybersecurity vs. Cyber Warfare
BY: ERIC CHABROW, GOVERNMENT INFORMATION SECURITY
09/23/2009
Army Lt. Col. Gregory Conti says that cybersecurity and cyber warfare are essentially the same, except that cyber warfare has “an offensive connotation.” Other terms, such as information assurance, information security or cybersecurity don’t have this connotation. West Point now includes a degree of cyber offensive training for cadets, who also complete two courses in cybersecurity. Conti says that West Point teaches their cadets cyber warfare from an “ethical perspective” and has won five of the nine National Security Agency cyberwar games that they have participated in.

Cyber Defense – Lots Going On
BY: KEVIN COLEMAN, DEFENSETECH.ORG
10/05/2009
National Security Agency Director Lt. Gen. Keith Alexander will become the United States’ first commander of the U.S. Cyber Command, which began its mission this month. However, questions still surround the USCYBERCOM’s mission and operations models. The creation of the command, along with other cybersecurity measures and expansions within governmental agencies, demonstrates the United States’ commitment to cybersecurity at a time where such threats increased three times in 2008. U.S. Intelligence Director Dennis Blair said in September nations such as China, Iran, North Korea and Russia have the skill to “challenge U.S. interests in traditional and emerging ways.”
http://www.defensetech.org/archives/005047.html

Collaborative Cyber Command
BY: KEVIN COLEMAN, DEFENSE TECH
09/28/2009
The article discusses the new Cyber Command and says that collaboration and coordination have been identified as significant challenges for the new command. The Joint Operations Center/Integrated Cyber Center will serve as the “nerve center” of the new command’s operations. An organizational chart for the new command shows a complex system of interactions that some believe could delay decision making and response from the new command. The article also discusses how collaboration and coordination should be given as much priority as “command, control, communications, computers, intelligence, surveillance and reconnaissance.”
http://www.defensetech.org/archives/005036.html

U.S. Cyber Command Goes Online
FROM: DEMOCRACY ARSENAL
10/01/2009
Editors from Democracy Arsenal are concerned with the secrecy associated with the new U.S. Cyber Command, which was set to go online Oct. 1. Concerns lie in USCYBERCOM’s mission, whom they will defend and what they will defend against. The editors continue by questioning whether the Pentagon’s actions will make the United States more cyberly secure or “provoke other nations to develop cyber warfare capabilities.”
http://www.democracyarsenal.org/2009/10/us-cyber-command-goes-online-.html
Military hackers could stop wars before they start
BY: MARTIN BRYANT, THENEXTWEB.COM
10/05/2009
Naval Postgraduate School professor John Arquilla has suggested a “nonlethal way to deter lethal conflict.” Such a plan recommends that the military hack enemy systems before they can begin cyber warfare. By doing this, enemies will rethink beginning a cyber war with the United States. Arquilla also suggests the U.S. work with global network specialists to “launch preemptive online strikes to head off real-world battles,” according to the article.
http://thenextweb.com/2009/10/05/military-hackers-stop-wars-start/

Lynn Calls for Collaboration in Establishing Cyber Security
BY: JIM GARAMONE, AMERICAN FORCES PRESS SERVICE
10/01/2009
While it may remain a new industry, all Americans must take cybersecurity seriously in order for the entire U.S. presence on the Internet to stay secure, said U.S. Deputy Defense Secretary William Lynn. Lynn said his department has faced threats from all types of perpetrators – teenage hackers, organized criminals and foreign spies – at “astonishing speed.” In order to deal with the multitude of cyber attacks, the DOD must work with other government agencies while ensuring civil liberties with defense systems.

Twitter is Mission Critical
BY: MAJ. DANIEL WARD, MAJ. GABE MOUNCE AND CAROL SCHEINA, SIGNAL CONNECTIONS
09/15/2009
The article says that the Defense Department’s decision to ban social media sites “isolates the defense work force from one of the biggest engines of social, economic and technological change in the world today.” Without access to social media, war fighters are also less able to collaborate and innovate, and the ban also causes issues for military technologists who develop and evaluate new technologies. The article discusses the three main reasons for blocking social media sites: maintaining assurance and security; regulating bandwidth; and governing employee time. Despite the Defense Department’s history of embracing new technologies, the department must recognize the many benefits of using social media.
http://www.afcea.org/signal/articles/templates/200909SIGNALConnections.asp?articleid=2069&zoneid=272
Web 2.0 Review Could Lead to Restricted Use of Social Networking in DoD
BY: DOUG BEIZER, FEDERAL COMPUTER WEEK
09/25/2009
Price Floyd, principal deputy assistant secretary of defense for public affairs, says that a recent review of the Defense Department’s use of social media will likely result in policies that allow the use of Web 2.0 tools, although some restrictions will be in place due to security concerns. Floyd explains that the review will examine the benefits of social media and the risks presented from social media sites, as well as the effect of social networks on the military’s operational security. Floyd also says that there will most likely not be a DoD-wide ban on social media.

All eyes on DOD’s social-media policies as review nears completion
BY: DOUG BEIZER, FEDERAL COMPUTER WEEK
10/01/2009
A Department of Defense spokesman said he expects the DoD’s review of using social networking sites in DoD agencies to recommend a policy with some restrictions and without entirely banning Web sites. The review of the benefits and risks associated with social networking sites is anticipated to be completed in October. Experts have said a total ban of social networking sites, such as Facebook and Twitter, wouldn’t work, and such sites do have potential benefits for the DoD. An expert in e-commerce and Web-based businesses said the DoD and other agencies should explain the security issues with social networking sites.

Pentagon Web 2.0 Strategy Could Give Spies, Geeks New Roles
BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
09/30/2009
A draft memo from the Defense Department includes new guidelines that would allow service members to use the DoD’s unclassified networks to access social networking sites, video hosting Web sites, blogs and Wikis. The memo says that troops can use these sites as much as they’d like, as long as they don’t claim to be representing the military or post images with their military uniform. The memo also says that it will be left to the Undersecretary of Defense for Intelligence to maintain threat estimates from “current and emerging Internet-based capabilities.”

Defense to Allow Troops, Family Members to Use Social Network Sites
BY: BOB BREWIN, NEXTGOV.COM
09/29/2009
The Defense Department will now allow troops and their families to use social networking sites and other online communication tools on its unclassified networks. A recent memo from Deputy Defense Secretary William Lynn III says that these sites are useful for both official and unofficial purposes and could provide an information advantage for defense. The DoD’s new policy on social networking says that these sites provide opportunities and also risks that will need to be balanced. The memo added that personal and unofficial use of “Internet-based capabilities” on the NIPRNET is permitted, but that users cannot claim to represent the department.
DoD Preparing to Lift USB Ban
BY: KELLY JACKSON HIGGINS, DARK READING
09/22/2009
Robert Cary, CIO for the U.S. Navy, recently reported that the Defense Department’s ban on USB devices will be lifted, although devices must be DoD-approved or procured. Cary says that Defense officials are working on the final policy for USB devices. Personally owned flash media devices will not be allowed, but devices that are “uniquely and electronically identifiable for use in support of mission-essential function on DoD networks” will likely be allowed for use by authorized individuals. Cary also reports that the Navy is working to become less dependent on USB flash media by using collaborative workspaces or file shares. The new Defense USB policy will be incorporated into USSTRATCOM guidelines.
http://www.darkreading.com/insiderthreat/security/storage/showArticle.jhtml?articleID=220100601

Should the Marines set up a cyber command?
BY: JASON MILLER, FEDERAL NEWS RADIO
10/06/2009
After the U.S. Army and Air Force have created cyber offices within their respective branches, the U.S. Marine Corps is now questioning its own cyberspace efforts, according to a FOUO paper. Currently, the USMC has a special program for cyber operations, but the FOUO paper discusses creating a single organization over the cyber operations. The Department of Defense is set to begin a departmental cyber command in October.
http://www.federalnewsradio.com/?nid=35&sid=1779288

U.S. Navy creates command to maintain cyber supremacy
FROM: AGENCE-FRANCE PRESS
10/02/2009
The U.S. Navy is creating an Information Dominance Corps in order to keep the United States advantaged in cybersecurity over adversaries, and the Navy hopes to have the reorganization completed by the end of 2009. A director of Information Dominance will head the group, and Vice Admiral Jack Dorsett has been nominated for the position. The Corps “will bring intelligence networks, electronic warfare, encryption operations, cyberspace communications and information gathering, as well as meteorology and oceanography, under a Fleet Cyber Command,” according to AFP.
http://www.google.com/hostednews/afp/article/ALeqM5g05UQUihfs3X-AGFirrDnlisQtqdtw
U.S. urges ‘cyber hygiene’ effort
BY: MAGGIE SHIELS, BBC NEWS
10/01/2009
As part of Cyber Security Awareness Month and its theme of “shared responsibility,” the U.S. Homeland Security Department has advocated that all Internet users perform good “cyber hygiene.” Experts within the cyber security field have focused on educating computer users about scams sent through e-mail, as it was recently reported that 87 percent of e-mail sent in August was spam. Phishing scams, often sent through e-mail spam, are now encroaching into social networking sites, and Facebook has acknowledged such scams in its blog. Security experts provide numerous ways to develop good “cyber hygiene,” which includes ensuring operating systems have up-to-date security systems, not opening e-mail attachments from unknown senders and avoiding clicking on links within e-mails.
http://news.bbc.co.uk/2/hi/technology/8279867.stm

Homeland Security to hire up to 1K cyber experts
BY: LOLITA C. BALDOR, ASSOCIATED PRESS
10/01/2009
The U.S. Homeland Security Department announced it will hire 1,000 new cyber experts by growing the number of cyber analysts, developers and engineers that work for DHS. These new employees will help “detect, investigate and deter cyber attacks.” Most of the money for the new positions has been budgeted, but the DHS continues to work with Congress to add money to its budget. DHS Secretary Janet Napolitano said the department doesn’t plan on filling all of the new positions.
http://www.federalnewsradio.com/?nid=33&sid=1776011

DHS Plans Cyber Job Fair
BY: BRITTANY BALLENSTEDT, NEXTGOV.COM
10/05/2009
The Department of Homeland Security will work with the Office of Personnel Management and the Office of Management and Budget to hold a job fair to fill the DHS’s 1,000 new cyber expert positions. The job fair will likely take place within four to six weeks, said CHCO Jeffrey Neal. The job fair will consider upper- to mid-level cybersecurity professionals, Neal said. He also said it could take up to three years to fill all the positions; regulations managing the application process for the 1,000 job openings are anticipated to be finalized this week.

Former DHS Cyber Czar Joins Wurldtech’s Advisory Board
DARK READING
09/23/2009
Greg Garcia, former Assistant Secretary for Cyber Security and Communications with the U.S. Department of Homeland Security, has joined the advisory board of Wurldtech Security Technologies, provider of the Achilles security analysis platform. Garcia will provide guidance on “strategic direction, business development, policy advocacy and other initiatives.” Tyler Williams, president of Wurldtech Security Technologies, says that Garcia is “one of the great minds in cyber security and critical infrastructure protection” and that Garcia will drive efforts to improve collaboration between public and private sector stakeholders.
http://www.darkreading.com/security/government/showArticle.jhtml?articleID=220101004
Cyberspace – International

**Singapore Beefs Up Cyber Security**
**BY: WENDELL MINNICK, DEFENSE NEWS**
10/05/2009
Singapore added a cybersecurity authority division to its Internal Security Department of the Ministry of Home Affairs Oct. 1. The Singapore Infocomm Technology Security Authority has a “mission to secure Singapore’s IT environment, especially vis-à-vis external threats to national security such as cyberterrorism and cyberespionage.” SITSA will work with numerous government agencies and offices in order to fulfill its missions with the public and private sectors.

**The Kremlin’s Eeeevil New Plan to Rein in Bloggers**
**BY: NATHAN HODGE, WIRED.COM**
10/01/2009
Russian President Dmitry Medvedev has hinted at a plan to censor what is published on the Internet. However, Medvedev wrote that, rather than one country making rules for the Internet, there should be international standards so that “we can counter terrorism, xenophobia and other unlawful activity on the Web.” Head of the pro-Kremlin party Sergei Mironov said in a speech Sept. 30 that there should be government censorship on some online material. Blogger Evgeny Morozov wrote that a “national consultative body,” such as the Russian Public Chamber, may decide the Internet rules and guidelines.

**Russian Cybergangs Make the Web A Dangerous Place**
**BY: JEREMY KIRK, NETWORK WORLD**
09/25/2009
Dmitry Samosseiko, a Sophos analyst, reports that Russian cybergangs are using affiliate networks, or “partnerka,” to direct users to fake Web sites that sell fake antivirus software, pharmaceuticals and counterfeit luxury products. Most of these affiliate networks require an invitation to join, and new recruits are given fake Web sites to promote. Criminals can infect computers through spam or by tampering with a computer’s DNS settings to direct users to fake Google sites which include malicious Web sites in search results. Sophos examined a popular partnerka called RefreshStats which uses Web sites that trick users into downloading a piece of malicious software. RefreshStats, as well as other affiliate networks, generally offer their users a commission for infected machines.

**Hackers Pay 43 Cents Per Hijacked Mac**
**BY: GREGG KEIZER, COMPUTERWORLD**
09/25/2009
Sophos researcher Dmitry Samosseiko recently discussed his investigation of a Russian affiliate network which found that Russian malware writers were offering hackers 43 cents for each Mac computer that they infected with bogus video software. Samosseiko says that the site, Mac-codec.com, is just one site dedicated to selling and promoting fake Mac software, proving that Mac users are not immune to the scareware threat. Graham Cluley, senior technology consultant at Sophos, says that Mac users could be more vulnerable to attacks than Windows users because they do not expect to be targeted by hackers and often do not have...
any anti-malware protection in place at all. The article also provides the link to download Samosseiko’s paper on Russian affiliate networks.


U.K. already ‘major world power’ in cyberwar
BY: CHRIS WILLIAMS, THE REGISTER
10/01/2009
The United Kingdom began its first national cybersecurity strategy in June, and British military and security services may need to look toward more unconventional recruiting techniques, said Scott Borg from the U.S. Cyber Consequences Unit. Borg called the U.K. a “major world power” in cyber warfare with its “considerable” amount of attackers and defenders. Former hackers could be used to defend U.K. networks.

http://www.theregister.co.uk/2009/10/01/borg_cyberwar/

New U.K. Cybersecurity Centre Opens Doors
DARK READING
09/23/2009
The new £30 million Centre for Secure Information Technologies (CSIT) was recently opened at Queen’s University Belfast’s Institute of Electronics, Communications and Information Technology and will use “the university’s international research expertise in high performance data and network security and intelligence surveillance.” The center will have to develop systems that can be used in next generation computer and telecom networks to provide better security than today’s PCs. Specifically, the centre will work on developing ultra high performance hardware-based cryptography systems that will improve data security and “pioneer the convergence of network, data and physical security” by developing new technologies. Recent research at Queen’s University is expected to be used in CSIT’s work to incorporate security in telecom and computer networks, especially in content-aware technology and real time traffic forensics.

http://www.darkreading.com/security/government/showArticle.jhtml?articleID=220101007

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.
‘State of the Internet’ assessed
BY: LANCE WHITNEY, CNET NEWS
10/01/2009
Akamai Technologies reported in its quarterly “State of the Internet” report that 133 more countries had used Internet attacks when compared to the first quarter. “The U.S., China and South Korea accounted for more than half of the attacks in the second quarter,” according to Whitney’s article. The report also found that overall, the global Internet connection speed dropped 11 percent to 1.5 Mbps. The United States was in the top 20 countries with fastest Internet connection, with an average speed of 4.2 Mbps.
http://news.cnet.com/8301-1009_3-10365091-83.html

Security Spending to Hit $14.5bn Says Gartner
TECHWORLD
09/23/2009
According to Gartner, the worldwide security software market will reach $14.5 billion in 2009, an 8 percent increase from 2008. Ruggero Contu, principal research analyst at Gartner, says that despite the economic downturn, security software will continue to be strong in 2009 because security is a critical area. Consumer security will be the largest segment of total software revenue in 2009, and Contu says that users are beginning to use “better-integrated multi-products, particularly in endpoint security, identity and access management.”

U.S. broadband lags Asian nations
BY: AARON SMITH, CNNMONEY.COM
10/01/2009
The United States wasn’t included in the top 10 countries providing quality broadband Internet services, according to a study done by business students at the University of Oxford-England and the University of Oviedo-Spain. South Korea was listed as No. 1 in the study, and Sweden was the top European country. The top three cities were in Japan, which was No. 1 in the study in past years. The study judged quality of broadband services by “measuring upload and download speeds, network latency and capacity.”

Prototype security software blocks DDoS attacks
BY: TIM GREENE, COMPUTER WORLD
10/05/2009
Researchers at Auburn University may have found a security method for DDoS attacks that could replace the current method of IP-address filtering. The method, termed Identity-Based Privacy-Protected Access Control Filter, has the “capability to resist massive denial of service attacks,” according to the researchers’ paper, while also reducing the amount of memory and CPU dedicated to differentiating between legitimate and illegitimate requests. Lead author of the paper, a professor of electrical and computer engineering at Auburn, said the researchers’ goal is to develop “a commercial version of the software for use in business networks,” though he isn’t sure when that could happen.
http://www.computerworld.com/s/article/9138982/Prototype_security_software_blocks_DDoS_attacks
Researchers Hijack a Drive-By Botnet
BY: ROBERT LEMOS, TECHNOLOGY REVIEW
10/02/2009
Researchers at the University of California – Santa Barbara conducted a four-month long study of “drive-by downloading” by connecting their server to computers associated with the Mebroot botnet. The researchers found that business Web sites were the most common to refer users “to a malicious download site,” though porn-hosting and illegal downloading sites were the most effective at redirecting users to the infected Web site, according to Lemos. Researchers also found that Mebroot uses “three different domain-generation algorithms, two of which only used the day’s date as an input.”
http://www.technologyreview.com/computing/23566/

Economic espionage
BY: BILL GERTZ, WASHINGTON TIMES
10/01/2009
A report from the Office of the National Counterintelligence Executive said foreign spies have been attempting “to steal economic and trade secrets” from U.S. Blackberries and iPhones. “Reports of new cyber attacks against U.S. government and business entities proliferated in fiscal year 2008,” according to the report that commonly mentioned Chinese espionage. Other Asian and Middle Eastern nations were mentioned in the report as the countries attempted to gain military and nuclear information through cyber espionage.
BY: TIM WILSON, DARKREADING
09/30/2009
Symantec’s MessageLabs unit conducted an analysis of several different botnets and reached multiple conclusions. One conclusion is that, despite earlier beliefs that the bigger the botnet network the larger the threat, botnet size isn’t necessarily relative to the amount of spam it can send out in one day. The leading botnet spam generator is Grum, which is half the size of the more commonly known Rustock botnet. Grum generates nearly 23 percent of the Internet’s spam with “an average of 39.9 billion spam messages per day last quarter.” MessageLabs also concludes in its report that 88 percent of the Internet’s spam is generated by botnets.

http://www.darkreading.com/securityservices/security/perimeter/showArticle.jhtml?articleID=220300610

Internet Has Never Been More Dangerous, Report Says
BY: THOMAS CLABURN, INFORMATION WEEK
09/30/2009
A report from the Anti-Phishing Working Group shows that from the fourth quarter of 2008 to June 2009, “phishing escalated to some of the highest levels we’ve ever seen,” said the group’s Chairman David Jevans. The number of detected fraudulent antivirus programs increased 585 percent, banking Trojans grew by 186 percent, phishing Web sites had its second-highest recorded amount with 49,084 and infected computers increased by about 66 percent from the beginning of the study to the end. Finjan also released a Cybercrime Intelligence Report that found some Trojans “have developed anti-forensic techniques to conceal account looting from automated anti-fraud systems and form the eyes of victims.”


Smart Grid Framework Vulnerable to Hackers – Report
BY: JAIKUMAR VIJAYAN, TECHWORLD
09/30/2009
The National Institutes of Standards and Technology (NIST) recently led a task force composed of government, industry and academic bodies, who looked into the security and privacy requirements for the U.S. Smart Grid. The draft report says that planners must address threats that could allow hackers to penetrate the smart grid and alter load conditions which could lead to widespread disruptions. Some say that the Smart Grid would have too many points of vulnerability into the network because of the software, wireless sensor networks and the Advanced Metering Infrastructure (AMI) networks. The report looks at vulnerabilities from malicious criminals as well as vulnerabilities caused by bad software coding, input validation errors and user authentication errors.


Research: Small DIY Botnets Prevalent in Enterprise Networks
BY: DANCHO DANCHEV, ZDNET
09/29/2009
A recent study led by Gunter Ollmann, vice president of research at Damballa, found that small botnets account for 57 percent of all botnets – most likely because smaller botnets are more likely to evade detection. Ollman says that while most people focus on larger botnets, smaller botnets are actually “more prevalent” in real-life enterprise environments. Smaller botnets are also more likely to be used for cyber espionage, as they can be “more specific
Scareware and Bots Require Layered Defenses
BY: JOHN SAWYER, DARK READING
09/23/2009
Author John Sawyer discusses the different reasons for increases in malware infections. Sawyer says that there are more cyber criminals now since most online crimes are used to make money instead of just fame or notoriety. Sawyer also discusses a recent report from NSS Labs on anti-malware products, and calls the report “disheartening.” Rick Moy, president of NSS Labs, says that users need multiple layers of protection to combat all of the new and rapidly changing attacks including Secure Web gateways, Microsoft User Account Control and whitelisting.


http://blogs.zdnet.com/security/?p=4485
Cyber Gangs Hit Healthcare Providers
BY: BRIAN KREBS, THE WASHINGTON POST
09/28/2009
In the past few months, organized cyber thieves have targeted healthcare providers, including non-profit organizations. For example, early in September cyber criminals stole $30,000 from the Evergreen Children’s Association – a non-profit organization that provides on-site childcare for public schools. Cyber criminals were also able to steal username and password information from Medlink Georgia Inc. – a not-for-profit health center that serves uninsured and under-insured patients. The criminals were able to transfer more than $44,000 from Medlink’s accounts to money mules that wired the funds to the criminals abroad. Last week, hackers stole almost $200,000 from Steuben ARC – a not-for-profit organization for developmentally disabled adults. The criminals had money transferred through 20 different money mules around the nation after stealing the company’s online banking credentials through a keystroke logging malware.

IRS Scam Now World’s Biggest E-Mail Virus Problem
BY: ROBERT MCMILLAN, NETWORK WORLD
09/25/2009
Gary Warner, director of research in computer forensics with the University of Alabama at Birmingham, says that a recent spam campaign is showing no signs of slowing down, and that this one campaign now accounts for 10 percent of all spam e-mail that his group is tracking. The spam was first detected Sept. 9 and has since sent millions of messages that include Trojan attachments or Web links to fake tax statements. The IRS warns users not to open attachments or links in e-mails that claim to be from the tax-collection agency. The malicious e-mails contain a version of the hard-to-detect Zeus Trojan, which hacks into bank accounts and steals money from victims.

‘Money Mule’ Recruitment Network Exposed
BY: BRIAN KREBS, THE WASHINGTON POST
09/24/2009
This article discusses a “money mule” that recently came forward to tell about the scam that she participated in. The mule, who remains anonymous, says that she was contacted by a company called Scope Group Inc. who said that they had found her resume on Careerbuilder.com. The company asked for extensive personal information from the woman, including bank account information and her social security number. The criminals then transferred money into the mule’s bank account, and instructed her to withdraw the money and transfer the funds to them through Western Union. The article provides screen shots of the images that the mule received from the criminals.

Massive E-mail Phishing Attack Hits Web
BY: CARL WEINSCHENK, ENTERPRISE SECURITY TODAY
10/06/2009
The scale of the phishing attack on a number of e-mail service providers is “incredibly rare,” said Mike Halsey, who operates a U.K. PC support site. PasteBin.com posted information on 20,000 subscribers to Microsoft’s Hotmail, MSN and Windows Live e-mail services online. On Oct. 6, PasteBin.com posted personal details of another 20,000 users of Gmail, Yahoo, AOL
Mail, Verizon and other e-mail service providers. A threat researcher at Panda Security said phishing attacks such as this “are often precursors to other initiatives.”

Hackers and Scalper Pounce on Google Wave Invites
BY: PATRICIA RESENDE, ENTERPRISE SECURITY TODAY
10/01/2009
The new Google Wave has become popular among those interested in trying the service and cyber criminals attempting to harm those that are interested. A security company has reported that some Google search results for Google Wave have links to fake antivirus offers created by hackers. A senior manager of the security company said Google searchers should pay attention to the link’s URL; don’t believe any Web site that says the computer is infected with a virus and keep the computer’s security up to date.

Soldiers’ Data Still Being Downloaded Overseas, Firm Says
BY: ELLEN NAKASHIMA, WASHINGTON POST
10/01/2009
Tiversa has found that unauthorized computers in foreign countries, such as China and Pakistan, have accessed and downloaded tens of thousands U.S. soldiers’ personal data that includes social security numbers, cell phone numbers, e-mail addresses, names of spouses and children and soldiers’ blood types. Tiversa found the data by using peer-to-peer file-sharing software, which was banned on Army computers in 2003 and later Pentagon and defense contractors’ computers. Critics, though, say the policies aren’t enforced.

Password-Stealing Malware Spikes
BY: JOHN SAWYER, DARKREADING
09/30/2009
McAfee’s blog reported “that password-stealing malware increased 400 percent in 2008,” and the numbers for 2009 are already nearly as much as the entire year of 2008. This exemplifies the growing trend of users’ passwords being stolen by malware. Certain malware types, such as Zbot, have been changing banking sites’ log-in pages to steal users’ information. Sawyer includes that the most targeted passwords are for gaming sites, but since most users are “manual-password synchronizers,” this could lead to more information being compromised.

PandaLabs: Record-Breaking 5 Million New Threats In Third Quarter Of 2009
BY: PRNEWswire, DARKREADING
10/01/2009
A PandaLabs report on the third quarter of 2009 showed that 71 percent of new malware from July to September were Trojans. Overall, the report showed that banking Trojans, adware and spyware account for the 5 million new types of malware. Computers infected with malware also increased by 15 percent when compared to the second quarter. The way malware was distributed through “spam, social networks and search engine optimization techniques” also increased in the third quarter.
New Trojan Gives Criminals Full-Service Bank Theft

BY: ROBERT MCMILLAN, COMPUTERWORLD
09/30/2009

Yuval Ben-Itzhak, Finjan’s chief technology officer, says that the new URLzone Trojan represents the “next generation of bank Trojans” and infected approximately 6,400 computers last month. The criminals behind the new Trojan, which was discovered by researchers at Finjan earlier this month, lure visitors to infected Web sites and then use a variety of PC software flaws to infect the visitors’ machines. Researchers say that the URLZone Trojan allows the criminals to set the system to make smaller withdrawals to avoid detection, and also changes the victims’ banking pages so that the transactions are not displayed.


Conficker Showdown: No End in Sight

BY: KELLY JACKSON HIGGINS, DARK READING
09/29/2009

Andre DiMino, director of the Shadowserver Foundation, says that the Conficker virus is still infecting machines and that researchers need to be more aggressive in stopping Conficker. Security researchers are concerned because Conficker continues to infect machines despite the resources and attention that have been “poured into eradicating Conficker.” Shadowserver says that there is no other threat that maintains the volume of infections that Conficker has, and Mikko Hypponen, chief research officer of F-Secure, says that it is very difficult to remove the botnet from infected machines. Researchers still do not know what the criminals behind Conficker are planning to do with the botnet, and the botnet has not yet been used for large distributed denial-of-service attacks like experts expected.

http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=220300359
Navigating the New Cybercrime Threatscape, Part 1
BY: JEFF DEBROSSE, TECHNEWSWORLD
09/09/2009
This article is the first part in a three-part series that explores cybercrime and cyber threats. This first article discusses the definition of cybercrime – crimes that exploit trust using a computer or traditional crimes carried out online. The target of cybercrime is usually information, which criminals expose or use to steal money. The article discusses the threat to Internet users from spam, viruses and worms. The article also examines phishing schemes, distributed denial-of-service attacks and botnets. Finally, the article looks at cyber crime as the “ultimate business plan” where criminals are financially motivated and the crimes are less risky. Most criminals are drawn to cybercrime because the legal system has not caught up to the growth of cybercrime, and because technological innovation is also a step behind new attacks and hacker techniques.

Navigating the New Cybercrime Threatscape, Part 2
BY: JEFF DEBROSSE, TECHNEWSWORLD
09/16/2009
The second article in this three-part series specifically discusses malware, botnets, phishing and data breaches. Malware, or malicious software, is usually used to steal money and is increasingly being distributed through botnets or networks of infected computers. Botnets work to infect as many computers as possible, and are then used in zombie networks to generate spam or participate in an attack. Phishing attacks are marketing scams that target a victim’s bank account information or private information by appearing to be a trusted source. Data breaches are another significant threat to users and usually result from weak passwords, unprotected transmission and under-protected internal networks.

Navigating the New Cybercrime Threatscape, Part 3
BY: JEFF DEBROSSE, TECHNEWSWORLD
09/23/2009
This article discusses cybersecurity practices that are helping to reduce the likelihood of becoming a victim of cybercrime. The OODA Loop – which stands for observe, orient, decide and act – is a strategy that helps victims establish a response plan for cybercrimes or attacks. Antivirus protection is an important part of cybersecurity, and most antivirus protection programs are now able to offer high performance and detection as well as low false-positive rates. The article also provides some best practices for cybersecurity, including using strong passwords; keeping systems updated and patched; verifying links in e-mails with the sending party; simplifying security for end-users; educating users; running network audits; and monitoring the devices on your network.

Battlefield High to host cyber security exercise
BY: AMANDA STEWART, INSIDENOVA.COM
10/01/2009
Area colleges, corporations, military groups and government organizations will compete in a two-day cyber warfare game called Cyber Dawn. The exercise will begin Oct. 3. Cyber Dawn has three goals, according to Tim
Rosenberg of White Wolf Security, the exercise’s organizer. First, it will bring together potential employers and employees. Second, participants will be able to test their cyber defense skills. Third, awareness of cyber security will be raised. The cyber attacks will be real but with systems that hold sample data, Rosenberg said.

http://www2.insidenova.com/isn/news/local/haymarket/article/battlefield_high_to_host_cyber_security_exercise/44391/

Hacker Conference Starts Next Week
THE STAR TECH CENTRAL
09/29/2009

Hacker Conference Starts Next Week
THE STAR TECH CENTRAL
09/29/2009

Hacker Conference Starts Next Week
THE STAR TECH CENTRAL
09/29/2009

Haroon Meer, technical director of information security company Sensepost, will speak at the 7th Annual Hack in the Box Security Conference, and will focus on the risk and vulnerabilities introduced by new technologies such as cloud computing. Meer will also discuss attacks that use cloud platforms. In another presentation, called “Offensive Cloud Computing with Hadoop and Backtrack,” the founder and CEO of Subterrain Networks Inc. Justin Lundy will discuss offensive techniques that utilize cloud computing. Sheran Gunasekera, head of R&D at ZenConsult, will demonstrate how criminals can spy on BlackBerry users and will discuss the release of the “Bugs and Kisses” toolkit for BlackBerry devices. The Hack in the Box conference will be Oct. 5 in Malaysia.


The Difficulty of Un-Authentication
BY: BRUCE SCHNEIER, THREAT POST
09/28/2009

Security expert Bruce Schneier discusses how companies continue to develop more forms of authentication, but that “unauthentication,” such as when a user leaves their computer logged in and running or turned on, also makes users vulnerable. Users can choose to have their system “time out” or log out automatically after a certain period of time, although this requires some “fine tuning” when choosing the appropriate amount of time to wait. Other systems use a USB authentication token that has to be plugged in for the computer to operate or an RFID token that logs the user out of the system when the token moves a certain distance from the machine. Schneier discusses the challenge of balancing usability and security on computer systems.

http://www.threatpost.com/blogs/difficulty-un-authentication-128

Microsoft Security Essentials Available for Download
BY: PATRICIA RESENDE, ENTERPRISE SECURITY TODAY
09/29/2009

Microsoft has made its Security Essentials antivirus software available as a free download in order to “remove cost barriers that leave PCs unprotected.” The software provides essential protection by targeting core features that most customers do not keep up-to-date without overusing system resources. Michael Gartenberg, an Interpret analyst, says that the new software is not a security suite, but that Microsoft wanted to make “install and forget” malware protection cheap for its users. Security essentials may be included in Windows 7 as its default antivirus software.


Sharing Threat Data is Key to Securing the Power Grid
BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NETWORK
09/24/2009

In this article, Seth Bromberger, director of the Energy Sector Security Consortium (EnergySec),
answers questions about the organization that helps with the exchange of security information among energy asset owners, industry and government. EnergySec is a non-profit organization that allows members to share information openly, without worrying about where the information will be disclosed. Bromberger says that EnergySec has improved security in the energy sector because members are more likely to share information. The organization also holds demonstrations of security products and techniques, as well as annual summits.


**Cyborgs for Cyber Defense**

BY: JART ARMIN, INTERNET EVOLUTION

09/28/2009

This article discusses how scientists at Sandia National Laboratories and researchers from the University of New Mexico’s Mind Research Network (MRN) are using neuroscience and systems engineering to learn how to better predict patterns of thought and behavior. The researchers hope that their study will track online enemies better using brain simulation, and develop a “human cyber team” that could work to prevent cyberwarfare and viral attacks. The MRN focuses on magnetic resonance imaging (MRI) and magneto-encephalography (MEG) in combination with computer modeling and simulation, brain simulation and genetic studies, and hopes that better interpretation of the cyber battleground will help more than analysis and modeling of previous behavior and attacks.


**Cyber Experts Learn from Ant Tactics**

TELEGRAPH.CO.UK

09/27/2009

The article discusses a new cyber defense strategy that is being tested by researchers at Wake Forest University in North Carolina. The researchers observed how ants behave when their colony was under threat, and are applying the same behavior to cyber defenders. The “digital ants” go through computer networks looking for invaders. If an invader is found by one “digital ant,” an army of other digital ants joins the fight to overwhelm the worm or virus. The researchers claim that this type of system will work better and faster than current models because invaders will be found faster, and the digital ants can resume their normal monitoring as soon as the worm or virus is defeated.


**VeriSign Embeds Authentication Into Cisco SA 500 Series Security Appliances**

DARK READING

09/26/2009

VeriSign Inc. recently announced that its VeriSign Indentity Protection (VIP) authentication will make small businesses more secure by making VIP credentials and two-factor authentication more affordable. VIP authentication functionality will now be included as part of the Cisco Small Business Pro SA 500 Series Security appliances, so small businesses can provide employees with remote access to VPNs while defending against Internet threats. Kerry Loftus, vice president of Consumer Authentication Solutions at VeriSign, says that VIP authentication is necessary for businesses to combat Internet attacks, and also says that implementing VIP and two-factor authentication is now easier and less costly.

http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=220300004
Lawmakers Weigh Government’s Role in Securing the Web
BY: LOLITA C. BALDOR, USA TODAY
09/28/2009
This article discusses how much control the federal government should have over the Internet, especially during a crisis. Melissa Hathaway, former White House cybersecurity advisor, says that there needs to be some system that can identify, isolate and respond to cyber attacks in the case of a “digital disaster.” There have already been 18 bills introduced in Congress that include provisions giving power to federal authorities to protect the nation in the case of a cyberattack, but the bills have all been controversial due to privacy concerns. Committee spokeswoman Jena Longo says that recent bills do not include giving the president the power to shutdown or take over the Internet, and that the president must maintain the power to direct the response to any crisis, including a cyber crisis. Privacy advocates continue to argue that the private sector can do a better job of securing networks than the government.

House Subcommittee Moves Bill to Boost Cybersecurity
BY: OTTO KREISHER, CONGRESSDAILY
09/24/2009
The House Science Research Subcommittee recently approved legislation that will require the Defense and Homeland Security departments and the National Science Foundation to establish long-term research and development programs that will authorize grants and scholarships for cybersecurity training. Rep. Daniel Lipinski (D-Ill.) and Rep. Eddie Bernice Johnson (D-Texas) say that the bill is the result of a series of hearings in which industry and government experts expressed a need for better coordination and research in cybersecurity, and will include provisions for better incentives for advanced cybersecurity studies.
http://www.nextgov.com/nextgov/ng_20090924_2618.php

Senators Plan Bill to Advance Net Neutrality
BY: CECILIA KANG, THE WASHINGTON POST
09/28/2009
Senators Byron L. Dorgan (D-N.D.) and Olympia J. Snowe (R-Maine) are considering legislation that would help to “advance the adoption of new rules on net neutrality.” The bill would set a timetable for the Federal Communications Commission to finish making net neutrality rules. The senators say that their bill would be similar to one released earlier in September by Representatives Henry Waxman (D-Calif.), Anna Eschoo (D-Calif.) and Ed Markey (D-Mass).

Cybersecurity Bill Pushes University-Business Alliances
BY: TIM GREENE, NETWORK WORLD
09/23/2009
The House Committee on Science and Technology’s Research and Science Education Subcommittee recently approved the Cybersecurity Research and Development Amendments Act of 2009, which would set up a scholarship program for cybersecurity students and establish summer cybersecurity internships in the federal government. A government task force is expected to form a plan that will prioritize research and development projects...
that will include private businesses and will also form a plan for building and maintaining an infrastructure to create, test and implement new secure networking and IT systems. The legislation also gives the president 180 days to outline the federal government’s cybersecurity staffing needs and how to meet them.


**House Panel Approves Cyber-Security R&D Bill**

BY: ROY MARK, EWEEK.COM
09/23/2009

A U.S. House subcommittee recently approved the Cybersecurity Research and Development Amendments Act of 2009, asking agencies to outline their cybersecurity role and determine the funding they will require to fulfill their specific research objectives. The bill also asks the National Science Foundation (NSF) to support new research on the social and behavioral aspects of cyber-security. The House Committee on Science and Technology’s Research and Science Education Subcommittee has held three hearings that examine federal cybersecurity including where progress is needed, the need for a more coordinated research plan and better partnerships between the private sector and government.


**Panel Passes Cyber Workforce Reform**

BY: BRITTANY BALLENSTEDT, NEXTGOV.COM
09/23/2009

The House Science and Technology’s Research and Science Education Subcommittee has passed a bill that “would strengthen the federal cybersecurity research and development portfolio” through better training for IT workers and improving partnerships between the government and private sector. The bill would also require federal agencies to provide details on their roles in cybersecurity and the funding they will require and the National Science Foundation will be required to support social and behavioral cybersecurity research. Rep. Eddie Bernice Johnson (D-Texas) is sponsoring an amendment that would make the Cyber Scholarship for Service program “more inclusive of minority students.”

## 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](#).

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Location</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Oct 2009</td>
<td>2nd Annual Cybersecurity Expo, Memphis, TN;</td>
<td><a href="http://cyberexpo.memphis.edu/">http://cyberexpo.memphis.edu/</a></td>
<td></td>
</tr>
<tr>
<td>20 – 22 Oct 2009</td>
<td>The 3rd International Conference on Cyberlaw, Beirut, Lebanon;</td>
<td><a href="http://www.conferencealerts.com/seeconf.mv?q=ca1mxx6m">http://www.conferencealerts.com/seeconf.mv?q=ca1mxx6m</a></td>
<td></td>
</tr>
<tr>
<td>4 – 5 Nov 2009</td>
<td>Dallas SecureWorld Expo; Dallas, TX;</td>
<td><a href="http://secureworldexpo.com/events/index.php?id=250">http://secureworldexpo.com/events/index.php?id=250</a></td>
<td></td>
</tr>
<tr>
<td>12 Nov 2009</td>
<td>SecureHouston, Houston, TX;</td>
<td><a href="https://www.isc2.org/EventDetails.aspx?id=4086">https://www.isc2.org/EventDetails.aspx?id=4086</a></td>
<td></td>
</tr>
</tbody>
</table>
### 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](#).

<table>
<thead>
<tr>
<th>Course Description</th>
<th>Provider</th>
<th>Dates and Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified Ethical Hacker</td>
<td>Global Knowledge</td>
<td><a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=10463&amp;catid=191&amp;country=United+States">Global Knowledge, Dates and Locations</a></td>
</tr>
<tr>
<td>Certified Secure Programmer (ECSP)</td>
<td>EC-Council</td>
<td><a href="http://www.eccouncil.org/Course-Outline/ECSP.htm">Online, EC Council</a></td>
</tr>
<tr>
<td>Certified VoIP Professional</td>
<td>EC-Council</td>
<td><a href="http://www.eccouncil.org/Course-Outline/ECVP.htm">Online, EC Council</a></td>
</tr>
<tr>
<td>CISA Prep Course</td>
<td>Global Knowledge</td>
<td><a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9416&amp;catid=191&amp;country=United+States">Global Knowledge, Dates and Locations</a></td>
</tr>
<tr>
<td>CISM Prep Course</td>
<td>Global Knowledge</td>
<td><a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9877&amp;catid=191&amp;country=United+States">Global Knowledge, Dates and Locations</a></td>
</tr>
<tr>
<td>CISSP Prep Course</td>
<td>Global Knowledge</td>
<td><a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=8029&amp;catid=191&amp;country=United+States">Global Knowledge, Dates and Locations</a></td>
</tr>
<tr>
<td>Computer Hacking Forensic Investigator</td>
<td>EC-Council</td>
<td><a href="http://www.eccouncil.org/Course-Outline/CHFI%20Course.htm">Online, EC Council</a></td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>Global Knowledge</td>
<td><a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11919&amp;catid=191&amp;country=United+States">Global Knowledge, Dates and Locations</a></td>
</tr>
</tbody>
</table>

---


17 – 18 Feb 2010 7th Annual Worldwide Security Conference, Brussels, Belgium; [http://www.conferencealerts.com/seeconf.mv?q=ca1m3m8x](http://www.conferencealerts.com/seeconf.mv?q=ca1m3m8x)


23 April 2010 Social Networking in Cyberspace, Wolverhampton, UK; [http://www.conferencealerts.com/seeconf.mv?q=ca1mh38](http://www.conferencealerts.com/seeconf.mv?q=ca1mh38)

17 July 2010 Cyberpsychology and Computing Psychology Conference (CyComP 2010), Bolton, Lancashire, UK; [http://www.conferencealerts.com/seeconf.mv?q=ca1mxia6](http://www.conferencealerts.com/seeconf.mv?q=ca1mxia6)
<table>
<thead>
<tr>
<th>Course</th>
<th>Provider</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Recovery</td>
<td>EC-Council, Online</td>
<td><a href="http://www.eccouncil.org/Course-Outline/Disaster%20Recovery%20Course.htm">http://www.eccouncil.org/Course-Outline/Disaster%20Recovery%20Course.htm</a></td>
</tr>
<tr>
<td>ESCA/LPT</td>
<td>EC-Council, Online</td>
<td><a href="http://www.eccouncil.org/Course-Outline/ECSA-LPT-Course.htm">http://www.eccouncil.org/Course-Outline/ECSA-LPT-Course.htm</a></td>
</tr>
<tr>
<td>Ethical Hacking and Countermeasures</td>
<td>EC-Council, Online</td>
<td><a href="http://www.eccouncil.org/Course-Outline/Ethical%20Hacking%20Countermeasures%20Course.htm">http://www.eccouncil.org/Course-Outline/Ethical%20Hacking%20Countermeasures%20Course.htm</a></td>
</tr>
<tr>
<td>Course Title</td>
<td>Provider, Format, Dates and Locations</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Risk Analysis and Management</td>
<td>Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11913&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11913&amp;catid=191&amp;country=United+States</a></td>
<td></td>
</tr>
<tr>
<td>SSCP Prep Course</td>
<td>Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9876&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9876&amp;catid=191&amp;country=United+States</a></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11941&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11941&amp;catid=191&amp;country=United+States</a></td>
<td></td>
</tr>
</tbody>
</table>
### 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](#).

<table>
<thead>
<tr>
<th>Office</th>
<th>Title</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLA Acquisition Locations</td>
<td>Information Technology (IT) Information Assurance Support and Management Services, Defense Distribution Center (DDC)</td>
<td><a href="https://www.fbo.gov/spg/DLA/J3/DDC/SP3300-09-R-0046/listing.html">https://www.fbo.gov/spg/DLA/J3/DDC/SP3300-09-R-0046/listing.html</a></td>
</tr>
<tr>
<td>PEO STRICOM</td>
<td>D--Threat Computer Network Operation (CNO) Teams for Test and Evaluation events</td>
<td><a href="https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=d713ee539a271238c8580dd6042731ea&amp;tab=core&amp;cview=0">https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=d713ee539a271238c8580dd6042731ea&amp;tab=core&amp;cview=0</a></td>
</tr>
<tr>
<td>Air Force Materiel Command</td>
<td>Integrated Cyber Defense &amp; Support Technologies</td>
<td><a href="https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=cd045a392c920683ccb0b03df09bb134&amp;tab=core&amp;cview=1">https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=cd045a392c920683ccb0b03df09bb134&amp;tab=core&amp;cview=1</a></td>
</tr>
<tr>
<td>Organization</td>
<td>Contract Information</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Air Force Materiel Command</td>
<td>D – NETCENTS-2 NETOPS and Infrastructure Solutions (Small Business Companion)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.fbo.gov/spg/USA/AFMC/ESC/FA8771-09-R-0019/listing.html">https://www.fbo.gov/spg/USA/AFMC/ESC/FA8771-09-R-0019/listing.html</a></td>
<td></td>
</tr>
<tr>
<td>Air Force Materiel Command</td>
<td>Security Certificate &amp; Accreditation Services for Information Systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.fbo.gov/spg/USA/AFMC/75/FA8201-09-R-0088/listing.html">https://www.fbo.gov/spg/USA/AFMC/75/FA8201-09-R-0088/listing.html</a></td>
<td></td>
</tr>
<tr>
<td>Air Force Materiel Command</td>
<td>A -- National Intelligence Community Enterprise Cyber Assurance Program (NICECAP)</td>
<td></td>
</tr>
<tr>
<td>Air Combat Command</td>
<td>A+, Network+, Security+ Training and Certification</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.fbo.gov/spg/USA/ACC/99CONS/F3G3FA9167AC02/listing.html">https://www.fbo.gov/spg/USA/ACC/99CONS/F3G3FA9167AC02/listing.html</a></td>
<td></td>
</tr>
<tr>
<td>United States Marine Corps</td>
<td>R--Internet Monitoring Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.fbo.gov/spg/DON/USMC/M67004/M6700409T0108/listing.html">https://www.fbo.gov/spg/DON/USMC/M67004/M6700409T0108/listing.html</a></td>
<td></td>
</tr>
<tr>
<td>Bureau of Industry &amp; Security</td>
<td>International Competitive Bidding (ICB): Implementation and Support of NATO Enterprise</td>
<td></td>
</tr>
<tr>
<td>Department of the Army</td>
<td>D--Information Assurance, Engineering System Solutions Development, Testing, Deployment and Life Cycle Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.fbo.gov/spg/USA/DABL/DABL01/W91QUZ-09-0000/listing.html">https://www.fbo.gov/spg/USA/DABL/DABL01/W91QUZ-09-0000/listing.html</a></td>
<td></td>
</tr>
<tr>
<td>Business Transformation Agency</td>
<td>Sources sought or request for information (RFI), DoD Information Assurance (IA) Controls (For Information Purposes Only)</td>
<td></td>
</tr>
<tr>
<td>National Aeronautics and Space</td>
<td>U--CISSP CERTIFICATION EDUCATION</td>
<td></td>
</tr>
<tr>
<td>Washington Headquarters Services</td>
<td>BAA - Research and Studies for the Office of Net Assessment (OSD/NA)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.fbo.gov/spg/ODA/WHS/WHSAPO/HQ0034-ONA-09-BAA-0002(1)/listing.html">https://www.fbo.gov/spg/ODA/WHS/WHSAPO/HQ0034-ONA-09-BAA-0002(1)/listing.html</a></td>
<td></td>
</tr>
</tbody>
</table>
EMPLOYMENT OPPORTUNITIES WITH NSCI

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

CYBERPRO CONTENT/DISTRIBUTION

Officers

President
Larry K. McKee, Jr.

Chief Operations Officer
Jim Ed Crouch

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.

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.

Please contact Lindsay Trimble regarding CyberPro subscription, sponsorship, and/or advertisement.

To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.

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