CyberPro

Volume 1, Edition 1
May26, 2008

Keeping Cyber Professionals Informed

Table of Contents

CyberPro

Volume 1, Edition 1
May26, 2008

Keeping Cyber Professionals Informed

** CYBER-RELATED CONFERENCES **

Note: Dates and events change often. The following is unofficial. Contact POCs for details.

If you have any additions/updates/suggestions for the CYBER calendar of events, please provide them to Larry McKee at mckeel@selectinnovation.com

20-21 May 2008	**AFCEA-George Mason University Symposium "Critical Issues in C^{4}I"**, George Mason University Johnson Center, Fairfax, VA (http://www.afcea.org/events/register.cfm?ev=14)
5-6 June 2008	**Space Security and Defense Conference: Critical Initiatives, Programs & Plans;** Washington DC; (http://www.asd-network.com/abm/abmc.asp?b=236&z=19)
9-10 June 2008	**Cyber Security Conference - Missions, Initiatives, Opportunities & Risks**, Washington DC, http://www.asdevents.com/event.asp?ID=238
16-20 June 2008	**Cyber Security for Process Control Systems Summer School**, At the Abbey Resort on Lake Geneva, Fontana, Wisconsin, (http://www.iti.uiuc.edu/events/SummerSchool2008.html)
17-18 June 2008	Enterprise Security Management Spring Forum, Bellevue WA, www.afei.org
17-19 June 2008	**Joint Warfighting 2008, "DoD Capabilities for the 21st Century"**, Virginia Beach VA, (http://www.afcea.org/events/east/08/intro.asp)
23-25 June 2008	**Space Warfare Symposium, "Space Situation Awareness and Command and Control: Keys to Future Global Security in Space"**, Keystone, CO -- (http://www.spacewarfare.org/)
24-27 June 2008	**Information Operations Europe 2008**, London UK (http://www.asdevents.com/event.asp?ID=215)
26-27 June 2008	**Identity Assurance: Authentication, Protection, and Federation**, Ronald Reagan International Trade Center, Washington, D.C. ***(***http://www.afcea.org/events/register.cfm?ev=17***)***
14-17 July 2008	**Annual International Test & Evaluation Association Technology Review**, Crowne Plaza Hotel, Colorado Springs, CO (www.itea.org)
15 – 17 July 2008	**Air Force Symposium 2008 – Cyberspace**, Maxwell AFB (Montgomery) AL (www.maxwell.af.mil/au/awc/cyberspace)
6-8 October 2008	**Strategic Space & Defense**, Qwest Center Omaha Convention Center and Arena, Omaha, NE, (http://www.stratspace.org/)

*** **OPEN-SOURCE MATERIAL** ***

Officials to explore cyberspace mission at symposium
AIR FORCE LINK
05/15/2008
The Air Force is hosting a symposium on service roles in cyberspace at Maxwell AFB in Montgomery, ALa. Air Force Symposium 2008 - Cyberspace will include topics such as defining and gaining control of cyberspace. Lt. Gen. Robert J. Elder Jr., Eighth Air Force commander will be a keynote speaker, as well as experts from the Department of Defense, commercial industry, and academia. General Elder states that the Cyber Symposium will be a defining event in the development of integrated air, space and cyber power.
http://www.af.mil/news/story.asp?id=123098860

Air University holds National Security Forum
BY: AIR UNIVERSITY PUBLIC AFFAIRS
05/15/2008
The Air University's Air War College's 55th Annual National Security Forum gives students the opportunity to discuss national security issues with leaders from across the nation, which is critical in enabling the students to lead future military operations. The event focuses on broadening student's perspectives and allowing dialogue between civilian guests and security experts, in order to increase public support for military operations. Michael Wynne, secretary of the Air Force, and Gen. T. Michael Moseley, Air Force chief of staff are featured speakers who will speak on current security issues that are affecting military forces.
http://www.au.af.mil/au/aupa/

Analysis: USAF's cyber offense capability
OKIE CAMPAIGNS
05/17/2008
The Broad Area Announcement from the Air Force Research Laboratory Information Directorate outlines a new effort to develop an offensive cyberwar plan that can combat enemy IT networks. Air Force spokeswoman Larine Barr emphasizes the importance of information technology in modern warfare, and the importance of staying on top of new technology. NATO announced that seven European nations will participate in a cyberdefense Center of Excellence in Estonia, which suffered a cyberattack last year.
http://okiecampaigns.blogspot.com/2008/05/analysis-usafs-cyber-offense-capability.html

Coalition to fight cyberterrorism
BY WADE-HAHN CHAN, FEDERAL COMPUTER WEEK
05/14/2008
The International Multilateral Partnership against Cyber-Terrorism (IMPACT) is a nonprofit program which includes participation from about 30 governments and multiple IT security companies to combat cyber crime. Howard Schmidt, a former chairman of the Critical Infrastructure Protection Board states that the IMPACT program will help give a more broad perspective on cyber crime. An IMPACT chairman reports that President Bush has expressed interest in US participation in the program.
http://www.fcw.com/online/news/152533-1.html

SASC on National cyber security initiative

SENATE ARMED SERVICES COMMITTEE REPORT 110-335
05/15/2008

The Senate Armed Services Committee reports on the administrations work to secure information networks in critical infrastructures. One concern over current initiatives is that almost all information available is highly classified, and unavailable to the public, which limits the amount of public education and debate. The committee also reported that more research, technology, and funds are needed for many elements of the administration's cyber initiative request in order to move the initiative out of the prototype or concept development phase. The committee also believes that many elements of the initiative are more focused on foreign intelligence collection, and that the cyber security elements of the initiative are actually modest.
http://vaphblueblog.blogspot.com/2008/05/on-national-defense-authorization-act.html

NATO to set up cyber warfare center

BY: ROBERT MCMILLAN, PC WORLD
05/14/2008

NATO is planning on establishing a cyber defense center in Estonia to help combat cyber warfare. Seven sponsoring European countries will provide half of the specialists on staff. Estonia suffered a widely reported cyber attack in May of 2007, which caused NATO to focus more on preventing and combating cyber attacks. Increased pressure from Allied defense ministers, as well as a request for help from Estonia has prompted NATO to form the cyber defense center, which will officially open in 2009.
http://www.pcworld.com/businesscenter/article/145916/nato_to_set_up_cyber_warfare_center.html

New technology proves to be dynamite during JEFX 08

MILCOM MONITORING POST
05/13/2008

The Air Force's F-22 demonstrated their potential for information-sharing technologies at the 2008 Air Force Joint Expeditionary Force Experiment. The F-22s were able to receive command messaging, imagery, updates and text messages into the cockpit through Tactical Targeting Network Technology (TTNT). TTNT is part of the of the Department of Defense's efforts to connect aircraft together and share information more efficiently. TTNT is only one of the potential information sharing systems that are being considered for Air Force aircraft. The technology will not be limited to F-22s but will hopefully connect all aircraft to enhance ISR and attack capabilities.
http://mt-milcom.blogspot.com/2008/05/new-technology-proves-to-be-dynamite.html

For next QDR, DOD to take leadership-driven approach

BY: BETTINA H. CHAVANNE, AEROSPACE DAILY & DEFENSE REPORT
05/13/2008

The Defense Department is using a new, leadership-driven approach to the next quadrennial defense review. Seven areas were identified for closer examination for the next QDR, including cyber and irregular warfare. The seven areas identified are the pressing issues that will be covered in the QDR, which begins in 2009 and is due in 2010.

Terror's new frontier: cyberspace
BY: TOM ALLARD, THE AGE
04/19/2008
The government is proposing new measures, including new laws, to counter threats to critical infrastructure from cyber attacks. Attorney-General Robert McClelland points out that the threat to critical infrastructures is very real and should be taken seriously. Cyber crime is rapidly becoming the new face of terrorist activity because it is harder to find who is responsible for the infiltration, and can paralyze commercial and government systems. Al-Qaeda has launched numerous cyber attacks already, all of which have proven to be hollow, but terrorists are rapidly seeking money and programmers to launch more sophisticated cyber attacks, aimed at obtaining sensitive security information.
http://www.theage.com.au/news/in-depth/terrors-new-frontier-cyberspace/2008/04/18/1208025468962.html

Air Force Colonel Wants to Build a Military Botnet
BY: KEVIN POULSEN, WIRED BLOG NETWORK
05/12/2008
Col. Charles W. Williamson III is proposing that the Air Force deliberately install DDoS code into its unclassified computer systems, as well as civilian government machines. Rob Kaufman, of the Air Force Information Operations Center, proposes installing botnet code onto the Air Force intrusion-detection systems. This would enable the Air Force to directly link counterattacks to systems that detect oncoming attacks.
http://blog.wired.com/27bstroke6/2008/05/air-force-col-w.html

FBI worried as DoD sold counterfeit networking gear
NETWORK WORLD
05/09/2008
The FBI Cyber Division is attempting to crack down on the distribution of counterfeit network hardware. A two year FBI effort, called Operation Cisco Raider, seized an estimated $3.5 million worth of counterfeit components manufactured in China. Fake Cisco routers were sold to the military and the FBI itself. The Defense Advanced Research Projects Agency is funding research programs to investigate how to better secure the global IT supply chain.
http://www.networkworld.com/news/2008/050908-fbi-worried-as-dod-sold.html

NSA Attacks West Point! Relax, It's a Cyberwar Game
BY: DAVID AXE, WIRED BLOG NETWORK
05/10/2008
The National Security Agency coordinated assaults on seven of the nation's military academies, including West Point, as part of the seventh annual Cyber Defense Exercise. The second rounds of attacks were aimed at highly protected networks, which are more difficult to combat. IT specialists were required to find the hijackers, scour the systems for unwelcome files and terminate them. Referees rated all seven of the universities defenses, and the Army once again placed over the Navy, Air Force, Coast Guard and others.
http://www.wired.com/politics/security/news/2008/05/nsa_cyberwargames

The Value of Space-Based Intelligence

BY: FRANK GARDNER, BBC NEWS
05/06/2008

The commander of US Strategic Command, Gen Kevin Chilton said that the ability to gather information and control operations from computers and satellite data was invaluable in the fight against terrorism in Iraq and Afghanistan. The four-star general also spoke on the new dangers of cyber warfare, and the ability of the Taliban to infiltrate computer systems and gain access to sensitive information. Operators under General Chilton's command have seen intrusions into the Pentagon's computer systems, which could point to sophisticated espionage by a foreign country. General Chilton feels that Iran specifically may be a potential threat for cyber security in the future.
http://news.bbc.co.uk/2/hi/americas/7386786.stm

Report: Government's Cyber Security Plan Is Riddled With New Spying Programs

BY: RYAN SINGEL, WIRED BLOG NETWORK
05/15/2008

President Bush's proposed $17 billion National Cyber Security Initiative may achieve less than expected. Many of the projects support intelligence gathering and analysis rather than focusing exclusively on cyber security. The initiative has been criticized for being highly classified, which would prevent the information from being available for education and public debate. The Armed Services Committee's analysis stated that the initiative involved a lot of spying under the guise of e-security. The National Security Agency is prepared to begin eavesdropping on the internet; accessing email, file transfers and Google searches without a warrant.
http://blog.wired.com/27bstroke6/2008/05/senate-report-g.html

Service Academies Vie for Cyber Cup

BY: HENRY S. KENYON, SIGNAL MAGAZINE
05/15/2008

In April, members from each of the military service academies participated in the 8th Annual Cyber Defense Exercise. The military academies combated simulated cyber attacks as a training exercise for future network administrators and security personnel. In order to make the simulation as realistic as possible, students designed a network, which was then attacked by NSA analysts and Army personnel. The teams were challenged with finding malicious software and removing or negating the malware. West Point won for the second consecutive year.
http://www.afcea.org/signal/default/

Air Force Aims for 'Full Control' of 'Any and All' Computers

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
05/13/2008

The Air Force would like to have access to hacker tools that would give them control over any type of computer there is. Various initiatives including "Cyberspace Command" and the $30 billion "National Cyberspace Initiative" aims to test cyber warfare techniques and technology to gain a better understanding of cyber security. The Air Force emphasizes that war used to require an army, but now can be done simply with an internet connection, and that the United States needs to be offensive concerning cyber security. The Air Force introduced a new effort, the "Dominant Cyber Offensive Engagement", a two year $11 million plan to put together hardware and software tools.
http://blog.wired.com/defense/2008/05/air-force-mater.html

Pentagon Wants Cyberwar Range to 'Replicate Human Behavior and Frailties'

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
05/06/2008

Pentagon researchers want to create an internet simulator to test out cyberwar tactics that replicates human behaviors in order to better prepare for online battle. The top secret $30 billion government-wide effort will create realistic chains of events, simulate multiple users, and even simulate use of physical devices such as a keyboard or a mouse. Darpa has already begun to contact potential contractors.
http://blog.wired.com/defense/2008/05/the-pentagons-w.html

White House Plans Proactive Cyber-Security Role for Spy Agencies

BY: BRIAN KREBS, WASHINGTON POST
05/02/2008

President Bush signed a directive in January authorizing intelligence agencies to monitor all federal network traffic in hopes of stopping hackers from stealing information or interrupting systems. The President's new directive will share information with the private sector, which is also vulnerable to attacks from hackers. This new plan comes five years after the President's released the National Strategy to Secure Cyberspace, which was left to the Department of Homeland Security to implement. Utilizing intelligence agencies will allow more information to be shared with the private sector, as well as provide more authority in the hopes of improving cyber security.
http://www.washingtonpost.com/wp-dyn/content/article/2008/05/02/AR2008050201646.html

Government enters the blogosphere

BY: JOHN ZYSKOWSKI, FEDERAL COMPUTER WEEK
05/12/2008

The government is now turning to online tools to gain public support and educate the public on government policies. Online tools are becoming increasingly effective. Blogging is the single most interactive web application available, and online tools can provide more interaction and participants. The Transportation Security Administration is now using online blogging to address public concerns and frustrations over TSA policies.
http://www.fcw.com/print/22_13/features/152474-1.html

Major cyberterrorism meeting scheduled

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
05/15/2008

The International Multilateral Partnership against Cyber-Terrorism (IMPACT) hosted the World Cyber Security Summit, which received support from more than 30 countries, including the United States. Malaysia provided a $30 million startup grant to fund the summit, which will focus on cyberterrorism, and developing an early-warning system which would monitor worldwide online activity. Russia and China, who have both posed cyberthreat to the United States, were among the participants in the summit. IMPACT expects a high level of cooperation from all of the countries involved, and emphasizes that all nations have an interest in cybersecurity.
http://www.gcn.com/online/vol1_no1/46265-1.html?topic=security&CMP=OTC-RSS

'Bot' Force Proposed as Cyber Weapon

MILITARY.COM
05/15/2008
An Air Force colonel proposes that the United States military build a "botnet" network similar to the networks that hackers use to disable online servers. The government's botnet would not harm innocent computers, but would be ready to attack computer networks of foreign enemies. The Air Force suggests using computers that would have been thrown away to build the botnet. Some criticize the plan, saying that the military botnet could accidentally attack innocent computers and that the best method of fighting cyberattacks is prevention and developing better methods of detecting incoming threats. Some security experts, however, argue that the botnet could be an effective cyberdefense tool provided the Air Force infected computers that they own.
http://www.military.com/news/article/bot-force-proposed-as-cyber-weapon.html?wh=news

Air Force Backtracks on Social Network Ban

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
05/16/2008
After banning the military themed social networking site, TogetherWeServed.com in January, the Air Force has released the restriction on the site after research has found that the site poses no security threat for the military. The Air Force continues to struggle with social media; the military bans many social networking sites that they believe to compromise military security, and then reverse the decision after further investigation into the sites. In one 2006 study, the Air Force moniterred official sites and operational security blogs, and found that the official sites were 65 times more likely to violate security rules than the social networking sites that are being targeted.
http://blog.wired.com/defense/2008/05/in-late-january.html

Air Force explains AFCYBER basing criteria for governors

MILITARYSPOT.COM
05/19/2008
The Air Force is in process of determining the final location for the Air Force Cyber Command. Governors will review basing criteria and provide suggestions, and then officials will meet with the community officials to determine the preferred location, as well as several alternate locations. The secretary of the Air Force expects to reach a decision by November 2008. The selection of the final location will be based on multiple criteria including capacity for growth, support from local businesses/universities, security levels and environmental hazards.
http://www.militaryspot.com/news/air-force-explains-afcyber-basing-criteria-for-governors/240

New IA centers to receive grants, scholarships

BY: WILSON P. DIZARD III, GOVERNMENT COMPUTER NEWS
05/19/2008
The Homeland Security Department and National Security Agency released the names of 23 universities who have been designated as National Centers of Academic Excellence in Information Assurance Research. The designated universities have the opportunity to apply for federal funds as well as scholarships through the Department of Defense Information Assurance Scholarship program. A majority of the schools included are located in the East, although the universities span 17 states and the District of Columbia.
http://www.gcn.com/online/vol1_no1/46302-1.html

What's in Lockheed Martin's wireless security lab?

BY: BRAD REED, NETWORK WORLD
05/20/2008

Lockheed Martin is currently conducting an evaluation of intrusion-detection devices, in order to report to the government which applications would provide the strongest defense against cyber intrusion. Lockheed Martin also conducts assessments of wireless networks before they go 'live' in order to suggest strategies and improvements for new government network defenses. Lockheed Martin is also developing new cyber-attack techniques, which could be used in future attacks against government networks, in order to find defensive strategies for developing attack methods.
http://www.networkworld.com/news/2008/052008-lockheed-martin-wireless-security-lab-side.html

Army aims to take guesswork out of cyberdefense

BY: WILLIAM JACKSON, GOVERNMENT COMPUER NEWS
05/20/2008

The Army Research Office is funding work by private companies to develop an early-warning system and database of security events, in order to increase the efficiency of cybersecurity tools. The Cyber-Threat Analytics (Cyber-TA) project, funded by the ARO, focuses on developing a program that could be used for commercial services as well as the military. The project has been funded through at least 2010; however, members of the Cyber-TA project state that there is still much work to be done at the core of cybersecurity.
http://www.gcn.com/online/vol1_no1/46306-1.html

Largest public power grid at cyber risk, feds say

BY: TIM GREENE, NETWORK WORLD
05/21/2008

The Tennessee Valley Authority, the nation's largest public electric company, does not comply with security guidelines recommended in a report published by the U.S. Government Accountability Office. The GAO states that unless the TVA implements security programs, they risk being victim to a cyber attack, which could interrupt service for the TVA's 8.7 million customers. The GOA privately laid out 73 recommendations for the TVA, but states that this is not a TVA specific problem, but rather an industry wide concern.
http://www.networkworld.com/news/2008/052108-power-grid-cyber-risk.html

SANS contributes funds, expertise to global cybersecurity group

BY: WILSON P. DIZARD III, GOVERNMENT COMPUTER NEWS
05/21/2008

The SANS Institute will contribute $1 million to IMPACT, as well as share technical information in the hopes of improving cyber security research in developing countries. The two groups will launch the Improved Cyber Defense through Cybersecurity Training and Skills Development activity, which will offer training in intrusion detection and penetration testing. The SANS Institute hopes to assist overseas academic institutions by equipping the schools with training and faculty skills.
http://www.gcn.com/online/vol1_no1/46326-1.html

CIOs look beyond Web 2.0

BY: JOHN COX, NETWORK WORLD
05/22/2008
Discussion at the fifth annual MIT CIO Symposium focused on the new and broadening applications and systems of Web 2.0. CIOs discussed the new importance of collaboration between systems, as well as the growing influence of social networking and virtualization. CIOs also discussed the problems associated with the new and more abstract forms of information sharing and system interaction.
http://www.networkworld.com/news/2008/052208-mit-cio.html

BLOG: 26 years after Gibson, Pentagon defines 'cyberspace'

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
05/23/2008
The Pentagon has redefined the meaning of cyberspace, which was released in a memo signed by Deputy Defense Secretary Gordon England on May 12. The new definition of cyberspace describes a "global domain" and includes all interdependent networks of information. The memo from England also stated that cyberspace is a "warfighting domain", and that the new definition will be the foundation for the Department of Defense to mature cyberspace security.
http://blog.wired.com/defense/2008/05/pentagon-define.html

Inside an FBI Computer Forensics Lab

BY: KEVIN POULSEN, WIRED BLOG NETWORK
05/23/2008
The FBI's newly accredited Regional Computer Forensics Lab in San Diego is one of 14 labs in the United States that solves crime by utilizing technology; retrieving evidence from computers, cell phones and memory cards. Photos from the inside of the San Diego lab are available at Wired.com.
http://www.wired.com/politics/security/multimedia/2008/05/gallery_computer_forensics

Cadet cyberwarriors head to AFIT

BY: ANN PATTON, AIR FORCE LINK
05/20/2008
Two Air Force cadets will soon be the first to go from the Air Force Academy to the Air Force Institute of Technology's cyber warfare program. AFIT has been teaching cyber-realted theories and technologies since the early 1990's and now offer courses in cryptography, information warfare and network security. AFIT, located on Wright-Patterson AFB in Ohio will continue to provide more graduate level cyber-education and research and believes that the field of cybersecurity will grow exponentially larger.
http://www.af.mil/news/story.asp?id=123099424

Lockheed gets $190M award for Joint Medical system's cybersecurity

AEROSPACE DAILY & DEFENSE REPORT
05/27/2008
Lockheed Martin will being providing the U.S. Navy's Space and Naval Warfare Systems Center with cybersecurity support as part of a five year contract worth up to $190 million. Lockheed Martin will provide technical services such as network operations/security, network defense, identify management and cryptographic repair and modernization.

http://www.aviationnow.com/search/AvnowSearchResult.do?reference=xml/aerospacedaily_xml/2008/05/27/06.xml&query=Lockheed+gets+%24190M+award+for+Joint+Medical+system%27s+cybersecurity *(log in required)*

Exposing the Information Domain Myth

BY: Major Geoffrey F. Weiss, USAF, AIR & SPACE POWER JOURNAL
03/01/2008

Major Geoffrey F. Weiss suggests that redefining information operations is essential in order to better train and equip forces to fight in traditional, as well as cyber domains. Major Weiss suggests that broadening the definition of IO is essential in educating and producing a more effective force across the "entire spectrum" of warfare, including the cyber domain.
http://www.airpower.maxwell.af.mil/airchronicles/apj/apj08/spr08/weiss.html

Dominant Cyber Offensive Engagement and Supporting Technology

05/12/2008

The Air Force Research Laboratory is accepting white papers for studies to increase our understanding of required capabilities and support for Dominant Cyber Offensive Engagement and Supporting Technology. Funded research is expected to result in complete functional capabilities in order to address the Dominant Cyber Offensive Engagement problem; however, smaller more focused studies will also be funded if they are found to be of "breakthrough" importance and quality. All applicants will be deemed potentially eligible and total funding is estimated to be $11 million. Complete criteria and information for submitting a proposal is including in the full length announcement.
https://www.fbo.gov/index?s=opportunity&mode=form&id=b34f1f48d3ed2ce781f85d28f700a870&tab=core&_cview=0&cck=1&au=&ck=

CyberPro Content/Distribution

This newsletter is intended to serve as a snapshot of Cyber-related events and issues, and is distributed every two to three weeks. Feel free to forward this newsletter to other interested individuals. If you have information you think should be included, or if you would like to be added or removed from distribution, please e-mail Larry McKee by clicking here Cyber Pro News Subscription.

The articles and information appearing herein are intended for educational and non-commercial purposes to promote discussion in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government or U.S. Department of Defense.