CyberPro

Volume 1, Edition 13
November 6, 2008

Keeping Cyberspace Professionals Informed

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 Larry McKee , ph. (757) 871-3578, 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 CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.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

Table of Contents **2**

Cyberspace – Big Picture **4**

Partnering for cyberspace security 4
Congress warms up to Web 2.0 4
Competing Against Israel 4
Joining Forces To Protect Cyberspace 5
United Nations plans cyber defense event 5
Security experts: Cyberattacks will increase 5
Agencies miss HSPD-12 target 5
ODNI establishes security center for embassies 5
Cybereye | Life in interesting times 6
Q&A: Mobile Forensics 6
Three ways Internet crime has changed 6
Internet coming to white space near you 7
Worry about browsers not OS, says Microsoft 7
Tech Group Battles Botnets 7
Routers at risk 7
SRA gets FAA cyber security deal 8
Northrop Grumman aligning with identity management systems 8
Network Forensics 8

Cyberspace and the New Administration **8**

Propelled by Internet, Barack Obama Wins Presidency 8
The Risks of a Digital Blindspot 9
Copyright and Politics Don’t Mix 9
Upcoming transition creates uncertainty 9
McCain, Obama IT reps face off 10

Cyberspace – Department of Defense (DoD) **10**

Mullen on cyberspace 10
Cyberspace Ops Defined 10
The Pentagon’s new wiki 10
DOD deepens Web 2.0 pool 11
DOD: Controlled but unclassified data is leaking 11
Pentagon moves quickly to install Microsoft patches, fend off cyberattacks 12

US Army warns of Twitter danger 12
The Official U.S. Army Chat Room Software 12
Navy encourages use of Web 2.0 tools 12
Air Force Aims to 'Rewrite Laws of Cyberspace' 12
Air Force cyber update 13
Cyber, Space work on merger details 13
BLOG: Air Force wants 'freedom to attack' online 13
Air Force leaders work to develop cyberspace roadmap 13
In new doctrine, Air Force eyes 'freedom of action' in cyberspace 14
Cyberspace – Department of Homeland Security (DHS) 14
DHS cybersecurity boss fights back against critics 14
Draft Cybersecurity Review Has Department on Defensive 15
Cyberspace Research 15
China top target for computer attacks: Microsoft 15
Cyber-criminals have easy ride in the UK 15
Microsoft: Software more secure, but malware is growing threat 15
Researchers show off advanced network control technology 16
Cisco study: IT security policies unfair 16
Internet Apps & Social Networking Office Boom Linked to Breaches 16
Cyberspace Hacks, Tactics, and Defense 16
New worm escapes into the wild 16
Q&A: Software Piracy 17
Keeping an Eye Out for the Sinowal Trojan 17
Advanced Radars Becoming Weapons With Cyber Bullets 17
State Department, VA disclose two new data breaches 18
Trojan virus steals bank info 18
IRAN: Hamas office declares cyber-war on Israel 18
Microsoft says Windows flaw could bring worm attack 18
US-Based Malware Network Shuts Down 19
Cyberspace - Legal 19
Think tank launches center on Internet policy issues 19
Can't Touch This 19
NZ teen convicted of cyber crime 20
Cyberspace-Related Conferences 20
CyberPro Content/Distribution 21

CYBERSPACE – BIG PICTURE

Partnering for cyberspace security

BY: WALTER PINCUS, WASHINGTON POST
11/03/2008

Donald Kerr, principal deputy director of national intelligence, delivered two speeches recently which called for better cooperation between government and the private sector to combat cyber threats. Kerr emphasized the importance of protecting government and private sector information in order to continue to develop advancements in science and technology. Kerr spoke at a symposium sponsored by the Office of the National Counterintelligence Executive about possible solutions including investment in technology and providing the same government protection capabilities to private industry sites. http://www.washingtonpost.com/wp-dyn/content/article/2008/11/02/AR2008110202204.html

Congress warms up to Web 2.0

BY: MICHAEL HARDY, GOVERNMENT COMPUTER NEWS
10/27/2008

Members of Congress are now allowed to set up profiles on social networking Web site Myspace.com which could help the adoption of other Web 2.0 tools. William McVay, executive vice president at G&B Solutions said the access to the social sites encourages Congress members to open discussions about Web 2.0 features. http://www.gcn.com/online/vol1_no1/47454-1.html?topic=&CMP=OTC-RSS

Competing Against Israel

STRATEGY PAGE
10/29/2008

The Hamas office in Iran has announced a hacking contest where contestants compete to make the most impressive attack on Israeli government agency or political Web sites for a $2000 prize. There are many Muslim skilled programmers and Internet specialists but many are either professionals in software and internet service companies and do not contribute much to cyber attacks. Many radical Muslims already participate in current Internet attacks between Sunni and Shia Muslims, but both Sunni and Shia Muslims support Hamas, which could unite the two groups against Israel. http://www.strategypage.com/htmw/htiw/articles/20081029.aspx

Joining Forces To Protect Cyberspace

FEDERAL BUREAU OF INVESTIGATION
10/24/2008

The article from the FBI offers some simple recommendations to help Internet users protect themselves online. Recommendations include: changing passwords regularly; signing up for cyber security alerts and tips; signing up for updates on the latest scams; joining local InfraGard chapters; and visiting the US-CERT website for information sharing. The article also provides the link to the FBI's cyber page for information about current projects and the link for the Department of Homeland Security page to find out about current cyber operations.
http://www.fbi.gov/page2/oct08/cyberprotections_102408.html

United Nations plans cyber defense event

BY: JOHN ANDREW PRIME, SHREVEPORT TIMES
10/30/2008

Joe Drew, spokesman for the Business Council for the United Nations recently announced the UN and the U.S. Air Force and Time Magazine will host "A Conversation about Cyber Defense", a global forum for international business leaders in New York City. Speakers include representatives from the U.S. Air Force, the FBI and the Department of Defense among others. The list of speakers is included in the article.
http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20081030/NEWS01/81029049

Security experts: Cyberattacks will increase

BY: WILLIAM MATTHEWS, AIR FORCE TIMES
11/04/2008

Georgia Tech University has published a report, called "Emerging Cyber Threats Report for 2009", on cyber threats that claim that cyberattacks will continue to increase, and will accompany almost all military action in the future. A group of security investigators, working as Project Grey Goose, reports that the cyberattacks against Georgia that corresponded with the Russian invasion of Georgia, was the work of nationalistic hackers and claim that the Russian government cannot be directly linked to the attacks, but does endorse cyberattacks. A Pentagon report released last spring claims that the biggest threat to the United States is not Russia, but China, and blamed China for intrusions into military computer systems.
http://www.airforcetimes.com/news/2008/11/airforce_cyberattacks_110408/

Agencies miss HSPD-12 target

BY: BEN BAIN, FEDERAL COMPUTER WEEK
10/31/2008

A report from the Office of Management and Budget found that less than a third of the identification cards that are required for federal employees and contractors under Homeland Security Presidential Directive 12 have been issued. The OMB had originally had an October 27 deadline for distribution, but only 12 agencies met the goal, with the majority of the distributed cards going to Department of Defense employees and contractors. The Office of Management and Budget recently provided recommendations to help agencies that are having implementation problems and emphasized the importance of the next presidential administration continuing the implementation effort.
http://www.fcw.com/online/news/154268-1.html?CMP=OTC-RSS

ODNI establishes security center for embassies

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK
10/31/2008

Under Intelligence Community Directive 707, the Office of the Director of National Intelligence has established the Center for Security Evaluation which will work with the State Department to help protect classified information from cyber intrusions. The Center

will work help improve national surveillance countermeasures and work with intelligence agencies to stop the security breaches in overseas U.S. embassies.
http://www.fcw.com/online/news/154260-1.html

Cybereye | Life in interesting times

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
10/27/2008

As a result of major initiatives including the Federal Information Security Management Act and presidential mandates concerning standardizing and updating IT resources, information security has become "better managed" and more organized. Author, William Jackson, believes that cybersecurity may see a budget cut in the 2009 federal budget which Jackson says is the result of the poor economy and the high cost of the wars. Jackson also says that cybersecurity is a good economic investment, but can take a significant amount of time to show a return.
http://www.gcn.com/print/27_27/47423-1.html?topic=security&CMP=OTC-RSS

Q&A: Mobile Forensics

BY: MIRKO ZORZ, HELP NET SECURITY
10/27/2008

In an interview with Help Net Security, Aviad Ofrat, the CEO of Cellebrite, answers questions about mobile forensics and the Universal Forensic Extraction Device. Questions covered many topics including: the importance of mobile forensics capability for law enforcement; the features of the Universal Forensic Extraction Device; and the challenges and advantages of the current marketplace. Ofrat also discusses how he hopes to see an increase of mobile device forensics in the future as well as advances in mobile device technology.
http://www.net-security.org/article.php?id=1184

Three ways Internet crime has changed

BY: JOAN GOODCHILD, COMPUTERWORLD
11/03/2008

Security products provider, Symantec, has released its biannual internet threat report which found that the biggest change in Internet security is the motivation behind cyber attacks. Cyber criminals are working less for notoriety or fame, and more for criminal intent and fraud, with a large increase in botnets which are very profitable for hackers. In the past, hackers tried to get more attention by attacking as many computers as possible, while hackers now aim to stay quiet and undetected for as long as possible. The report also found that the United States and China are consistently the top worldwide targets for cyber attacks and that most hackers now target individual Internet users.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9118882&source=rss_topic82

Internet coming to white space near you

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
11/05/2008

The Federal Communications Commission has adopted rules that allow wireless service providers to use "white space" that is currently part of the television RF spectrum for high-speed Internet access. Wireless providers are expected to being using the unused spectrum in coordination with the move of television broadcasters to new bands with the requirement of using digital signals in February. Service providers as well as equipment manufacturers feel the decision will provide broadband access to more consumers as well as stimulate investment, near-term economic growth, and national competitiveness. Devices that will use the white space spectrum must be FCC approved and certified.
http://www.gcn.com/online/vol1_no1/47506-1.html

Worry about browsers not OS, says Microsoft

BY: JOHN E. DUNN, TECHWORLD
11/03/2008

Microsoft's latest Security Intelligence Report found that nine out of ten software vulnerabilities target applications, while the number of vulnerabilities that target operating systems is decreasing. The report also found that 42 percent of Windows XP vulnerabilities come from Microsoft software, making XP the most vulnerable platform. Finally, results showed that China was the most vulnerable location with 46.6 percent of exploits, while the United States came second with 23 percent of the exploits.
http://www.techworld.com/news/index.cfm?RSS&NewsID=106453

Tech Group Battles Botnets

BY: BRAD REED, NETWORK WORLD
11/02/2008

The Messaging Anti-Abuse Working Group (MAAWG), which includes ISPs and Internet companies, are scheduled to meet in February in San Francisco to work towards a strategy for combating botnets, which have been increasing in popularity for DDoS attacks. The MAAWG hopes to develop at least a list of best practices as well as discuss how to deal with infected machines and educate users on cleaning machines. At the last meeting in September, the group formed a subcommittee which will work on the set of best practices for ISPs and a committee which will study the switch to IPv6 and its affect on the detection and prevention of botnet attacks.
http://www.pcworld.com/businesscenter/article/153121/tech_group_battles_botnets.html

Routers at risk

BY: DAN CAMPBELL, GOVERNMENT COMPUTER NEWS
10/31/2008

Rapid Internet expansion has caused some routers in the Internet routing table to be overwhelmed with information, and in danger of breaking down. Some routers are not up to performance or memory requirements which put their networks at risk of melting down. Most large ISPs and enterprises have already upgraded their networks and will not be affected by some routers failing. The article explains that most routers have previously been fine because the growth of the Internet routing table has been gradual, but the table will soon reach a "tipping point" that will hurt some routers.
http://www.gcn.com/online/vol1_no1/47476-1.html

SRA gets FAA cyber security deal

BY: WILLIAM WELSH, WASHINGTON TECHNOLOGY
11/03/2008

The Federal Aviation Administration has awarded a $56 million, five year contract to SRA International Inc. who will work with the Transportation Department on cyber security needs. SRA will work with the Cyber Security Management Center to help protect the Transportation Department, the Federal Aviation Administration and other companies from cyber threats. The article includes other companies that will work with SRA to improve cyber attack prevention, detection and response capabilities.
http://www.washingtontechnology.com/online/1_1/33852-1.html/

Northrop Grumman aligning with identity management systems

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK
10/30/2008

Northrop Grumman has announced it will issue identification cards that comply with federal standards to aerospace and defense employees, and will be one of the first contractors to implement a centralized public-key infrastructure. Northrop Grumman encourages other federal contractors to develop identify management programs which, like the OneBadge cards, coordinate with the Defense Department and federal policies. Defense contractors are also addressing global supply chain cyber threats.
http://www.fcw.com/online/news/154248-1.html

Network Forensics

JOHN H. SAWYER, DARK READING
10/23/2008

NetworkMiner, a “Network Forensic Analysis Tool for Windows” provides users with connection information between IP addresses that could be useful in forensic investigations. Some advanced network forensics products record all network traffic to provide more detailed information on the user’s activity. NetworkMiner is free and is able to provide user credentials, do fingerprinting of operating systems and extract media files from FTP, HTTP and SMB. NetworkMiner is one of many emerging tools that provide network analysis, file recovery and tracking which are all feature of “network forensics”.
http://www.darkreading.com/blog.asp?blog_sectionid=447&doc_id=164343&WT.svl=blogger1_1

CYBERSPACE AND THE NEW ADMINISTRATION

Propelled by Internet, Barack Obama Wins Presidency

BY SARAH LAI STIRLAND, WIRED BLOG NETWORK
11/04/2008

Barack Obama’s use of the internet to find volunteers, donations and support proved to be a large part of his victory in the election. Obama’s website helped supporters organize campaign events and brought in a significant portion of the Obama campaign’s total $600 million in contributions. The Obama campaign worked with Facebook co-founder Chris Hughes to build a social networking site, myBarackObama.com, and used text messages to reach young voters. Obama is not the first to use the Internet in a campaign, but Ralph Benko of Capital City Partners in Washington, D.C. believes the campaign serve as an example of using technology in future electioneering.
http://blog.wired.com/27bstroke6/2008/11/propelled-by-in.html

The Risks of a Digital Blindspot

BY: JOHN PALFREY, HARVARD LAW SCHOOL BLOG
10/31/2008

Palfrey discusses the differences between "BlackBerry-toting" Barack Obama and "self-described computer illiterate" John McCain, and the importance of having a leader that is comfortable with advancing technologies. Obama's campaign used the Internet to reach young voters, ask for donations and organize volunteers. A familiarity with the Internet and other advancing technologies is important to many of the top issues of the election including surveillance of terrorists, protection of civil liberties and cybersecurity.
http://blogs.law.harvard.edu/palfrey/2008/10/31/the-risks-of-a-digital-blindspot/

Copyright and Politics Don't Mix

BY: LAWRENCE LESSIG, THE NEW YORK TIMES
10/20/2008

Digital technologies have played significant roles in the 2008 Presidential election, enabling voters to debate issues, respond to arguments and voice opinions, which has resulted in copyright laws being misused for censorship. The article briefly discusses some examples including: Fox News forcing John McCain to stop using a clip of a Fox News-moderated debate; Warner Music Group requiring YouTube to remove political videos that included its music; and NBC requesting that Barack Obama stop airing an ad that contained NBC News video. By claiming to be a victim of copyright infringement, the corporations "are effectively censoring political speech". Many are calling for reform of copyright laws and removing the law from unnecessary contexts.
http://www.nytimes.com/2008/10/21/opinion/21lessig.html?_r=1&oref=slogin

Upcoming transition creates uncertainty

BY BRIAN ROBINSON, FEDERAL COMPUTER WEEK
09/22/2008

James Lewis of the Center for Strategic and International Studies said that he is concerned about the Comprehensive National Cybersecurity Initiative being stalled during the transition to the new presidential administration. Both McCain and Obama acknowledge the importance of cyber security, and Obama lists cybersecurity as one of his top five priorities and said he would even appoint a federal chief technology officer to oversee government efforts. Amit Yoran of netWitness Corp. said that the CNCI would be evaluated and recommendations would be reported to the new administration. One major recommendation from the Commission for Cybersecurity for the 44th Presidency would be to give control of many cybersecurity projects to the White House National Security Council.

http://www.fcw.com/print/22_31/features/153840-1.html?CMP=OTC-RSS

McCain, Obama IT reps face off

BY: WYATT KASH, GOVERNMENT COMPUTER NEWS
10/28/2008

Technology representatives for both presidential candidates spoke at the American Council for Technology and Industry Advisory Council's Executive Leadership Conference about how the candidates would handle various information technology issues. Michael Nelson, a professor of Internet studies at Georgetown University, represented the Obama campaign. Tim Hugo, executive director of the Free File Alliance, represented the McCain campaign. Questions addressed many topics including: the role of contractors; the importance of government transparency; the priority of cybersecurity; the reform efforts of the next president; and improvements to information sharing.
http://www.gcn.com/online/vol1_no1/47460-1.html?topic=&CMP=OTC-RSS

CYBERSPACE – DEPARTMENT OF DEFENSE (DOD)

Mullen on cyberspace

INSIDE THE PENTAGON
10/30/2008

At an Air Force base in Alabama, Chairman of the Joint Chiefs of Staff Adm. Michael Mullen expressed concern over military leaders' lack of familiarity with the "cyber world" and said that it is important to be educated and informed in order to make good decisions for cyber security. Mullen also said that he feels that there is not enough organization and that security issues go far beyond the military and affect the entire Internet.

Cyberspace Ops Defined

BY BOB BREWIN, GOVERNMENT EXECUTIVE
11/03/2008

A September memo from Marine Gen. James Cartwright to Deputy Secretary of Defense Gordon England redefined cyberspace operations as using cyber capabilities for military objectives in or through cyberspace, including computer network operations and defense of the Global Information Grid. The article discusses how defining cyberspace operations is important in developing a foundation for the military to better prepare for cyber warfare as well as develop a unified joint cyber command. The article also briefly discusses the Defense Information Systems Agency's decision to allow workers who do classified work to work from sensitive compartmented information facilities (SCIF) in the Northern Virginia Area, although they have not had offers of available SCIFs that were not outrageously expensive.
http://www.govexec.com/story_page.cfm?filepath=/dailyfed/1108/110308wb.htm

The Pentagon's new wiki

BY: DOUG BEIZER, GOVERNMENT COMPUTER NEWS
11/05/2008

The Department of Defense has launched a wiki called Techipedia, which is similar to Wikipedia, in order to improve collaboration among military service members, scientists, engineers and acquisition workers. Techipedia was launched on October 1 in an effort to better help warfighters by supporting coordination in science and technology investments. The wiki is available to federal employees and contractors, and the DoD is planning to launch an external version in the coming months to connect federal employees with industry.
http://www.gcn.com/online/vol1_no1/47505-1.html

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

DOD deepens Web 2.0 pool

BY DOUG BEIZER, FEDERAL COMPUTER WEEK
10/31/2008

The Department of Defense will soon be using wikis, blogs and Web 2.0 tools to improve communication between Department employees and warfighters. DoD Techipedia, which was modeled after the Web site Wikipedia and launched on October 1, will improve communications among the military service members and agency employees, and will hopefully coordinate the Department's $10 billion a year science and technology work. An external version is expected to be available soon. Other Web 2.0 tools are also expected to improve communications between the DoD and warfighters by offering easier accessibility and user friendliness.

http://www.fcw.com/online/news/154267-1.html

DOD: Controlled but unclassified data is leaking

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK
10/27/2008

In a recent memo, DoD Chief Information Officer John Grimes said that some controlled unclassified information is publicly accessible from Defense Department sites, and discussed the importance of protecting the sensitive information. The Army has formed a Defense Industrial Base Cyber Security Task Force which will evaluate security risks and work to develop policies that will focus on companies in areas including: command and control; systems modernization; development and testing facilities; supply chains; and communications and intelligence programs.

http://www.fcw.com/online/news/154195-1.html?CMP=OTC-RSS

Pentagon moves quickly to install Microsoft patches, fend off cyberattacks

BY BYRON ACOHIDO, USA TODAY
11/01/2008

In a presentation at the National Defense Foundation's cyber symposium in Colorado Springs, Rear Admiral Jan Hamby announced that the Pentagon is working quickly to install the Microsoft Windows patch on all military workstations and computer servers that use Microsoft. Hamby controls information security for both the North American Defense Command and NORTHCOM. Hamby also said that there has been a large increase in attempts to penetrate military networks and that many social networking and high traffic sites have been blocked from military computers. Hamby also explained that the Pentagon has worked to improve cyber security since the 2005 attack on U.S. military systems by Chinese hackers, and said that as our systems become more resilient, we come closer to a better deterrence effect.

http://blogs.usatoday.com/technologylive/

US Army warns of Twitter danger

BY: JIM REED, BBC NEWS
10/27/2008

A U.S. Army report draft voiced concerns that emerging mobile and web technologies could be used to encourage extremist ideas and propaganda and said that tools such as satellite navigation and mapping devices have already been discussed by al-Qaeda. Leaders in the United States and the UK are worried that popular social sites like Facebook, MySpace and Twitter could be used by terrorists. The British government is even proposing heavier surveillance of mobile and Internet systems. Privacy advocates and anti-terror experts have protested the idea of storing phone and Internet records.

http://news.bbc.co.uk/newsbeat/hi/technology/newsid_7693000/7693050.stm

The Official U.S. Army Chat Room Software

STRATEGY PAGE
11/05/2008

The U.S. Army is installing the new Green Force Tracking software, an army version of IBM Lotus Sametime, which will allow troops to communicate through encrypted Internet connections especially officers and troops that are going to combat zones to replace other troops. The "off-the-shelf software" is cheaper for the military because of "commercial roots" and is expected to make communication essential for technical support, information about supplies and combat zone expectations easier.

http://www.strategypage.com/htmw/htiw/articles/20081105.aspx

Navy encourages use of Web 2.0 tools

BY: DOUG BEIZER, FEDERAL COMPUTER WEEK
10/28/2008

A memo by Robert Carey, the Navy's chief information officer, said that the Navy encourages the use of Web 2.0 tools including wikis, blogs and Web feeds to help improve communication and provide information and easy access to troops. Carey wrote that the tools must still not violate current policies and cannot compromise sensitive information. Carey also emphasized the impact that Web 2.0 tools could have on information sharing and collaboration.

http://www.fcw.com/online/news/154217-1.html

Air Force Aims to 'Rewrite Laws of Cyberspace'

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
11/03/2008

The Air Force Research Laboratory recently announced the "Integrated Cyber Defense" program which aims to rewrite the "laws of cyberspace" by blocking hostile traffic from Air Force networks, identifying previously anonymous hackers, and working towards enabling Air Force servers to dodge cyber attacks. Rick Wesson, CEP of security firm Support Intelligence warns that the Air Force can control its own networks and laws, but cannot completely rewrite the laws of the Internet. Still, the Air Force aims to eliminate many threats by securing vulnerabilities before they are exploited. Donald Hanson, Information Directorate chief, said military networks may be able to be made inaccessible to malicious traffic, and also explained that the Air Force should work more towards dodging potential attacks than trying to shut every attack out. http://blog.wired.com/defense/2008/11/air-force-aims.html

Air Force cyber update

BY: JENN ROWELL, MONTGOMERY ADVERTISER (ALA.)
10/31/2008

Since the decision to cancel the Air Force Cyber Command, the Air Force is moving forward with a Numbered Air Force under Air Force Space Command which will be a smaller organization than the original Cyber Command. Ed Gulick, a AF spokesman, explained the 24th Air Force is expected to release a roadmap in early December, and will include some of the original plans for the Cyber Command. In response to recent problems with nuclear operations, the Air Force is also considering a major command which will oversee nuclear operations. http://www.montgomeryadvertiser.com/apps/pbcs.dll/article?AID=200881031035

Cyber, Space work on merger details

BY: ERIK HOLMES, AIR FORCE TIMES
10/28/2008

Maj. Gen. William Lord explained that the Program Action Directive would provide a plan for the merge of the provisional Air Force Cyber Command and Air Force Space Command, and would probably go into effect next spring. Author, Erik Holmes, says that the move will be the largest reorganization since the disbanding of Strategic Air Command in the early 1990's. Air Force Cyber Command will change to the 24th Air Force and will operate under the Air Force Space Command. Lord said that the Cyber Command and Space Command had much in common, especially in areas of expertise, and expects the 24th Air Force to include around 6,000 personnel. http://www.airforcetimes.com/news/2008/10/airforce_cyberspace_merge_102808/

BLOG: Air Force wants 'freedom to attack' online

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
10/24/2008

According to the "Cyberspace Operations – Air Force Doctrine Document 2-11," the Air Force wants "freedom of action" on the Internet including the "freedom from attack and freedom to attack." According to the document, cyberspace operations would include the ability to deceive enemies and use the cover of natural events to jam enemy equipment. Airmen would also be able to disrupt terrorist communications over the Internet by exploiting and destroying Internet links, and by sending terrorists false information or e-mails. http://blog.wired.com/defense/2008/10/in-new-doctrine.html

Air Force leaders work to develop cyberspace roadmap

AIR FORCE LINK
10/24/2008

Air Force leaders at Barksdale AF Base in Louisiana are continuing work to develop a plan for combining the Air Force Cyber Command and the Air Force Space Command following the announcement that the Air Force Cyber Command was replaced by a numbered Air Force with a focus on "cyberspace warfighting operations". The former AFCYBER team is

helping with developing the plan and is also assisting with updating the Program Action Directive which will define which units will focus on cyberspace missions. Maj. Gen. William T. Lord said that the two domains have a lot in common, and will be more powerful together. Lord also explained that the Space Command will oversee cyber operations and provide training and resources.
http://www.af.mil/news/story.asp?id=123121153

In new doctrine, Air Force eyes 'freedom of action' in cyberspace

INSIDE THE AIR FORCE
10/24/2008

The Air Force will reportedly release the “Cyberspace Operations – Air Force Doctrine Document 2-11” later this year which would add “freedom of action” a key policy in cyberspace. An early draft of the Document described cyberspace freedom of action as “freedom from attack and freedom to attack” and also acknowledges the challenges of both offensive and defensive capabilities in the cyberspace domain. The document also contains a broad plan for Air Force cyber operations. AF spokesman Charles Gulick said the document would be ready for release within weeks.

Cyberspace – Department of Homeland Security (DHS)

DHS cybersecurity boss fights back against critics

BY: JOHN LEYDEN, THE REGISTER
10/29/2008

Homeland Security undersecretary Robert Jamison, who oversees the Department’s cybersecurity efforts, defended the Department’s work on improving cyber security, saying the Department had improved its systems’ defenses against attacks and would continue to carry out plans for improving security. The DHS has also made progress by eliminating thousands of entry points into government networks and developing Einstein 2, an intrusion detection program. Jamison also said that the criticism of the DHS shows a lack of understanding of the DHS’s current work and plans for the future, and that the proposed leadership reorganization would stall the Department’s progress.
http://www.theregister.co.uk/2008/10/29/dhs_cybersecurity/

Draft Cybersecurity Review Has Department on Defensive

BY: CHRIS STROHM, NATIONAL JOURNAL
09/22/2008

A commission from the Center for Strategic and International Studies and the Homeland Security Department disagree over who should be in charge of federal computer network security. The DHS was originally given control of securing civilian and some private sector networks following Bush's cybersecurity initiative but some argue that there is still no clear leadership, and the commission is still unsure what role the DHS should play in cybersecurity. Robert Jamison, undersecretary for Homeland Security's national protection and programs directorate, said that the DHS has made progress in cybersecurity by reducing access points and developing intrusion detection devices. The DHS also requested that the commission meet with DHS staff before issuing a final report which will provide recommendations about cybersecurity to the next president.
http://www.nationaljournal.com/congressdaily/cdp_20080922_3512.php

CYBERSPACE RESEARCH

China top target for computer attacks: Microsoft

SPACE WAR
11/03/2008

Microsoft released a security report which evaluated cyber threats and vulnerabilities, and found that China is the preferred target of attacks that hide malicious programs in Web browser applications. The report found that 47 percent of software exploits from the first half of the year were in Chinese, and only 23 percent were in English. The study also found that more of the vulnerabilities were ranked "high severity" than the same period in 2007, and that the majority of the online attacks were from "Trojan Horses" which hide malware in downloaded programs. Microsoft recommends keeping operating systems and software current and updated to avoid the viruses.
http://www.spacewar.com/reports/China_top_target_for_computer_attacks_Microsoft_999.html

Cyber-criminals have easy ride in the UK

BY: CARRIE-ANN SKINNER, TECHWORLD
11/03/2008

Research by the Corporate IT Forum found that 69 percent of 35,000 surveyed businesses have experienced some cyber crime and 68 percent of companies spend as much as 40 percent of their security budgets on cyber security. The survey also found that only four percent of the businesses would report security breaches and 57 percent feel that the United Kingdom Government would handle incident reports properly.
http://www.techworld.com/news/index.cfm?RSS&NewsID=106452

Microsoft: Software more secure, but malware is growing threat

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
11/03/2008

Microsoft recently released the fifth biannual Microsoft Security Intelligence Report which evaluated vulnerabilities, exploits and threats including those not exclusive to Microsoft software. The report found that software vulnerabilities dropped by 4 percent since the last report but that the amount of malware and unwanted software found on computers had jumped 43 percent. The report concluded that the increase of Trojan viruses is indicative of the increasing use of botnets for organized crime. The article contains other findings from the

report as well as a summary of recommendations for computer users to better protect themselves.
http://www.gcn.com/online/vol1_no1/47485-1.html

Researchers show off advanced network control technology

BY: TIM GREENE, NETWORK WORLD
10/30/2008

A new technology, OpenFlow, is still in the concept stage but hopes to boost bandwidth and save power in business networks. OpenFlow would allow users to define flows and choose the path through the network. The technology was demonstrated at the Global Environment for Network Innovation (GENI) Engineering Conference in Pal Alto, Calif. The demonstration showcased some of the technologies capabilities through a network between California and Japan.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9118579&source=rss_topic17

Cisco study: IT security policies unfair

BY: JIM DUFFY, NETWORK WORLD
10/28/2008

Cisco recently released the results of the second part of a worldwide study on data leakage. The second report focuses on the behaviors that put corporations at risk of data breaches. The study surveyed more than 2,000 employees and IT professionals in various countries and found that half of the employees admitted to breaking their corporate security regulations. Most of the employees that broke the security rules called the policies unfair and many believe that some policies would keep them from performing some job duties. The article also recommends that IT departments improve communication and policy awareness.
http://www.networkworld.com/news/2008/102808-cisco-security-policies.html

Internet Apps & Social Networking Office Boom Linked to Breaches

BY: KELLY JACKSON HIGGINS, DARK READING
10/28/2008

FaceTime Communications Inc. conducted a survey of IT managers that found that 60 percent reported their employees using social networking sites at the office. The organizations that started using the social networking sites recently reported an average 39 security incidents a month while organizations that used social networking sites less reported around 23 incidents a month. The survey also reported that almost 100 percent of the responding organization's employees use at least one site like Facebook, YouTube or instant messaging. FaceTime's vice president of marketing and product management, Frank Cabri, said that a third of the employees surveyed would violate IT policies by using the applications, and Cabri recommends reaching a compromise with employees to allow limited access while blocking harmful features.
http://www.darkreading.com/showArticle.jhtml?doc_id=166788&WT.svl=news1_1

CYBERSPACE HACKS, TACTICS, AND DEFENSE

New worm escapes into the wild

BY: GREGG KEIZER, COMPUTERWORLD
11/04/2008

Symantec's security response team has announced that a worm, which Symantec calls "Wecorl", is capable of exploiting a vulnerability just patched by Microsoft. Kevin Haley, a director of the security team, believes the worm may have originated in China and is different than the Trojan horse that originally prompted the Microsoft patch on October 23. Once behind the firewall of one Windows PC, the worm attacks all other machines on the same subnet, which is particularly important for companies that have many laptops configured to the same location where parts of firewalls are disabled. Symantec rated the worm as a "very low" threat and Microsoft has reportedly issued an emergency patch. http://www.techworld.com/news/index.cfm?RSS&NewsID=106484

Q&A: Software Piracy

BY MIRKO ZORZ, HELP NET SECURITY
11/03/2008

Help Net Security interviewed Jan Samzelius, the CEO and co-founder of ByteShield, an organization which works to prevent illegal copying of software applications and games. Questions covered many topics including: countries most affected by software piracy; law enforcement; the strengths and weaknesses of current anti-piracy software; the future of piracy threats; and the future of anti-piracy projects and software. http://www.net-security.org/article.php?id=1186

Keeping an Eye Out for the Sinowal Trojan

BY: BRIAN PRINCE, EWEEK.COM
11/03/2008

RSA, the security division of EMC, has observed at least 60 different versions of the Sinowal Trojan each month over the past six months, and found information from almost 300,000 online banking accounts as well as credit account information and other personal information. Many of the virus' versions are not detected by security software such as Symantec or McAfee. The Trojan, which targets Windows 2000, XP, and Vista, uses HTML injection to redirect Internet users to fake websites which ask for log-in or financial information. RSA has chosen not to publish a list of affected financial institutions, but have alerted both the companies and law enforcement. http://www.eweek.com/c/a/Security/Keeping-an-Eye-Out-for-the-Sinowal-Trojan/?kc=rss

Advanced Radars Becoming Weapons With Cyber Bullets

BY: DAVID FULGHUM, AEROSPACE DAILY & DEFENSE REPORT
11/05/2008

The U.S. Air Force has awarded a $238 million development and demonstration contract to Boeing and Raytheon for the development and testing of an advanced radar for the Strike Eagle fleet of 224 aircraft. The active electronically scanned array (AESA) radar will be both a sensor and weapon and will allow integration of software electronic warfare packages. The new technology would allow the radar to pick out very specific targets such as vehicles or humans

walking, and would identify the people and vehicles with their communications, which would more accurately identify the targets in a large battlefield.
http://www.aviationweek.com/aw/generic/channel_.jsp?channel=aerospacedaily

State Department, VA disclose two new data breaches

BY: JAIKUMAR VIJAYAN. COMPUTERWORLD
11/03/2008

The U.S. Department of State and the U.S. Department of Veterans Affairs have both announced data security breaches for the second time this year. The Department of State reported that information for almost 400 individuals had been stolen from a database intrusion, and the Department of Veterans Affairs announced a medical center in Oregon accidentally posted personal information on 1,600 patients on its public Web site. According to the State Department, the records were accessed by an employee who was since terminated, and all those affected were notified by the Department. The VA data breach, in which information on patients was reportedly loaded to a federal Web site that publishes details of government contracts and spending, is only one of many recent embarrassing security breaches for the VA.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9118959&intsrc=hm_list

Trojan virus steals bank info

BY MAGGIE SHIELS, BBC NEWS
10/31/2008

The company RSA, which works to improve network security for Fortune 500 companies, have been tracking the Sinowal Trojan virus which is reported to have stolen information from 500,000 online bank and credit card accounts worldwide. RSA's Fraud Action Research Lab has been following the Trojan since February 2006 and found data breaches in multiple countries including the United States, the United Kingdom, Australia and Poland. Interestingly, no Russian accounts were affected by the virus. RSA reports the virus is particularly dangerous because Internet users can be infected without knowing by visiting a Web site that contains malicious code. RSA recommends Internet users be cautious when visiting high traffic Web sites such as social networking sites and also reminds users not to provide social security numbers or other personal information online.
http://news.bbc.co.uk/2/hi/technology/7701227.stm

IRAN: Hamas office declares cyber-war on Israel

BY: RAMIN MOSTAGHIM, LOS ANGELES TIMES
10/25/2008

A Palestinian political group recently announced that it would award cash prizes to hackers who can penetrate a "Zionist" website. Hamas announced the contest at a media expo in Tehran. Israeli hackers recently loaded the Israeli national anthem onto a hacked Hamas website, and a few years ago, a group of Israeli hackers broke into a Hamas website and redirected the traffic to a pornography site. The winner of the hacking contest will receive $2000, and contest organizers have said that the competition is a "peaceful and non-violent initiative".
http://latimesblogs.latimes.com/babylonbeyond/2008/10/iran-hamas-offi.html

Microsoft says Windows flaw could bring worm attack

BY: ROBERT MCMILLAN, NETWORK WORLD
10/23/2008

Microsoft recently released an emergency patch for a flaw in Windows that they announced could be used in a large worm attack. If the flaw was exploited, the hackers

would be able to install malicious programs and create new accounts and would also have access to user data. Businesses that use local area networks would be particularly vulnerable because of a lack of firewall protection. The attack code for the hack had not been publicly released, but Microsoft released the emergency patch to avoid any serious security breaches from the flaw.
http://www.networkworld.com/news/2008/102308-microsoft-says-windows-flaw-could.html

US-Based Malware Network Shuts Down

BY: TIM WILSON, DARK READING
09/22/2008

Atrivo, an ISP similar to the Russian Business Network, was formerly one of the largest carriers of hacker information and exploits but is reported to be no longer operating. Robert Graham, CEO of Errata Security, said the site was probably shut down by law enforcement or suffered a network failure. Graham also warns that the end of Atrivo will probably not have much impact of malware and hacks as Atrivo users will find another ISP to use, and believes that Atrivo could easily be restarted under a different name.
http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211201236

CYBERSPACE - LEGAL

Think tank launches center on Internet policy issues

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
10/23/2008

The Progress and Freedom Foundation recently launched the Center for Internet Freedom which supports advancing technologies, Internet user education and self-regulation instead of government regulation. The increasing dependence of U.S. communications and commerce on the Internet, many regulatory issues are going to the Federal Trade Commission, the Federal Communications Commission and Congress. These regulatory issues related to privacy rights, liability issues, and freedom of speech concerns are increasing the pressure on the government to provide “protection and regulation”. Berin Szoka, a director of the center, said that government regulation would slow Internet innovation and diminish “free market and property rights”.
http://www.gcn.com/online/vol1_no1/47410-1.html

Can't Touch This

BY: MICHAEL ISIKOFF & MARK HOSENBALL, NEWSWEEK
10/23/2008

The inspectors general of U.S. intelligence agencies are required by Congress to provide a public report on President Bush’s “warrantless-surveillance program” , which is due July 2009. The inspectors general recently produced the first interim report to Congress, but made the document classified which sparked protests from House Intelligence Committee Chairman Silvestre Reyes. Reyes claimed Congress was expecting a document that could be available to the public, and also requested an order which would stop any documents related to the surveillance program from being destroyed. The program has caused controversy since President Bush first had the National Security Agency start surveillance of suspected terrorist communications without warrants after 9/11.
http://www.newsweek.com/id/165235

NZ teen convicted of cyber crime

BBC NEWS
04/01/2008

Owen Thor Walker, 18, of New Zealand was convicted of six charges of "using computers for illegal purposes" after the police found that the group Walker belonged to had infiltrated more than one million computers and stolen over $20.4 million from online bank accounts. Walker designed a virus that anti-virus software did not detect, and used the virus to steal log-in information and credit card details. Walker was arrested as part of the FBI's global botnet investigation last November.
http://news.bbc.co.uk/2/hi/asia-pacific/7323733.stm

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.

13-14 Nov 2008	**Information Assurance for DoD and Homeland Defense,** Washington, DC, http://www.asdevents.com/event.asp?ID=328
3-4 Dec 2008	**FinSEc 2008,** Palm Beach Gardens FL, http://www.misti.com/default.asp?page=65&Return=70&ProductID=7474
11-12 Dec 2008	**European Conference on Computer Network Defense,** Dublin Ireland, **http://2008.ec2nd.org/ec2nd/597-EE.html**
19-21 Jan 2009	**International Workshop on e-Forensics Law,** Adelaide Australia, http://www.e-forensics.eu/
26-29 Jan 2009	**U.S. Department of Defense Cyber Crime Conference,** St Louis MO, http://www.dodcybercrime.com/9CC/
16-19 Feb 2009	**Black Hat DC 2009,** Washington DC, http://www.blackhat.com/
9-11 Mar 2009	**INFOSEC World Conference & Expo,** Orlando FL, http://www.misti.com/default.asp?page=65&Return=70&ProductID=5539
13-15 Mar 2009	**Cybercultures: Exploring Critical Issues,** Salzburg Austria, http://www.inter-disciplinary.net/ci/Cyber/cybercultures/c4/fd.html
30 Mar – 2 Apr 2009	**Computational Intelligence in Cyber Security,** Nashville TN, http://www.ieee-ssci.org/index.php?q=node/21
6-8 Apr 2009	**Cyber Security and Information Intelligence Workshop,** Oak Ridge National Laboratory, http://www.ioc.ornl.gov/csiirw07/
14-17 Apr 2009	**Black Hat Europe,** Amsterdam The Netherlands, http://www.blackhat.com/
20-24 Apr 2009	**RSA Conference,** San Francisco CA, http://www.rsaconference.com/2009/US/Home.aspx
24 – 28 May 2009	**Internet Monitoring and Protection,** Venice Italy, http://www.iaria.org/conferences2009/SECURWARE09.html
14 – 19 Jun 2009	**International Conference on Emerging Security Information, Systems and Technologies;** Athens Greece, http://www.iaria.org/conferences2009/SECURWARE09.html
15-19 Jun 2009	**Air Force Cyberspace Symposium 2009,** Bossier City, Shreveport, LA, http://www.cyberinnovationcenter.org
25-30 July	**Black Hat USA 2009,** Las Vegas NV, http://www.blackhat.com/
7-10 Jul 2009	**Conference on Ubiquitous Intelligence and Computing,** Brisbane Australia, http://www.itee.uq.edu.au/~uic09/
17-19 Aug 2009	**DFRWS (Digital Forensics Research) 2009 Annual Conference,** Montreal Canada, http://www.dfrws.org/2009/

CyberPro Content/Distribution

Officers

President
Larry K. McKee, Jr.

Senior Analyst
Jim Ed Crouch

CyberPro Research Analyst
Kathryn Stephens

CyberPro Archive

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 Larry McKee , ph. (757) 871-3578, regarding CyberPro subscription, sponsorship, and/or advertisement.

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