CyberPro

National
Security
Cyberspace
Institute
NSCI

Keeping Cyber Professionals Informed

Officers

President
Larry K. McKee, Jr.

CyberPro Research
Analyst
Kathryn Stephens

This newsletter is intended 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 shall not be used 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 other appropriate administrative, civil, and/or criminal action.

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest. 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.

Table of Contents

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

CyberPro   *National Security Cyberspace Institute*   **Page | 1**

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

CyberPro   *National Security Cyberspace Institute*   **Page | 2**

** CYBER-RELATED CONFERENCES **

Note: Dates and events change often. Please visit web site for details.

Please provide additions/updates/suggestions for the CYBER calendar of events here.

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
2 – 7 Aug 08	**Black Hat USA 2008 Briefings & Training**, Caesars Palace, Las Vegas, NV, http://www.blackhat.com/
15-17 Sept 2008	**24th Annual Air & Space Conference and Technology Exposition**, Washington D.C., http://www.afa.org
18-19 Sept 2008	**Current and Future Military Data Links**, Washington D.C., http://www.asdevents..com/event.asp?ID=257
25-26 Sept 2008	**Electronic Warfare Operations and Systems 2008**, London UK, http://www.asdevents.com/event.asp?ID=241
30 Sept – 2 Oct 2008	**National Security 2008**, Brussels, Belgium, http://www.asdevents.com/event.asp?ID=265
6-8 Oct 2008	**Strategic Space & Defense**, Qwest Center Omaha Convention Center and Arena, Omaha, NE, http://www.stratspace.org/
7-9 Oct 2008	**2008 Cyber Awareness Summit**, Bossier City-Shreveport, LA, http://www.cyberinnovationcenter.org/
16-17 Oct 2008	**8th Annual C4ISR Integration Conference** , Defense News Media Group, Arlington, Virginia, http://www.dnmgconferences.com/07c4isr/index.php?content=home

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

CyberPro   *National Security Cyberspace Institute*   **Page | 3**
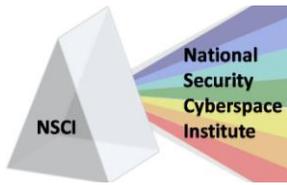
*** OPEN-SOURCE MATERIAL ***

Cyberspace career fields, training paths, badge proposed

BY: KAREN PETITT, AIR FORCE LINK

07/02/2008

Maj. Gen. William T. Lord, the Air Force Cyber Command commander, announced at a recent cyberspace symposium that enlisted and officer corps will be trained in establishing, controlling and fighting in the cyberspace domain. Cyber warriors will be grouped into four categories: operators, specialists, analysts and developers. The Air Force "roadmap" for cyberspace will also outline education and training paths, and General Lord also proposes a badge that will identify future cyber operators.

http://www.af.mil/news/story.asp?id=123105049

Security Researchers: Not the Enemy

DARK READING

07/01/2008

Security researchers, who are often responsible for finding the vulnerability in corporate websites, are often mistreated, as companies fear public disclosure of security weaknesses. For example, Google, who does have a good track record in security, does not recognize security researches that identify holes in their security systems. Microsoft, however, holds security conferences, and asks researchers to communicate with the company about security problems. Security researchers provide a valuable service to many companies, and can offer assistance with identifying security flaws.

http://www.darkreading.com/blog.asp?blog_sectionid=403&doc_id=157993&WT.svl=blogger1_1

Censoring the Internet: It's a wrongheaded way to prevent terrorism

INFORMATION WARFARE MONITOR

07/02/2008

Sen. Joe Lieberman believes that terrorist threats from the Internet are imminent, and proposes that terrorist messages on the internet should be censored from the American public. Lierberman recently requested that YouTube remove all videos that were produced by groups listed as U.S. State Department "Foreign Terrorist Organizations" such as al-Qaeda, and YouTube agreed to remove 80 videos.

http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1892&mode=thread&order=0&thold=0

Public institutions' Web sites target of cyber-attacks

DAILY YOMIURI ONLINE/ASSOCIATED PRESS

07/02/2008

Japanese websites have been the victims of a series of cyber attacks by SQL injections. The attacks hack into servers and set up programs that infect the sites with computer viruses, and the hackings are currently being investigated by the National Police Agency. On May 29, a suspicious log was found in a Takamatsu municipal government server which connected the site to a Chinese web site which was programmed to infect users' computers. Two other attacks have been made this year on Japanese websites, all by SQL injection, but it is believed that the attacks were meant to alter the websites, and not steal information.

http://www.yomiuri.co.jp/dy/national/20080702TDY03305.htm

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

CyberPro   *National Security Cyberspace Institute*   **P a g e | 4**
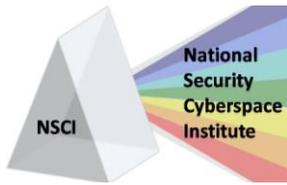
NIST issues guidelines to test agencies' network security

BY: JILL AITORO, NEXTGOV

07/01/2008

The National Institute of Standards and Technology released guidelines on Monday to evaluate how well computer systems defend against cyberattacks, which explain how to evaluate a network's controls, risk management process, and security strengths and weaknesses. The recommendations include penetration testing, which are supervised breaches of security controls with appropriate hardware/software tools to find security vulnerabilities, incorrect system configurations and architectural weakness, as well as a log of activity.

http://www.nextgov.com/nextgov/ng_20080701_4388.php

Service Aims to Master Threats before the Bad Guys

BY: RITA BOLAND, SIGNAL

06/16/2008

The Air Force Research Laboratory at Wright-Patterson Air Force Base is developing the Virtual Combat Environment for Electronic Conflict (VCEEC), which will prepare the Air Force and other services for a wide range of threats through simulation and virtual combat training. VCEEC will support testing and evaluation of sensor technologies, electronic warfare concepts, cyberspace and information operations concepts and research tools. The Air Force has awarded contracts for VCEEC to work with Booz Allen Hamilton and Northrop Grumman Mission Systems.

http://www.afcea.org/signal/articles/templates/signal_connections.asp?articleid=1632&zoneid=220

Collaboration Key to Network Warfare

BY: HENRY KENYON, SIGNAL

07/01/2008

The Joint Information Operations Warfare Command (JIOWC), which is part of U.S. strategic command (STRATCOM), is working to integrate information operations into the U.S. military's planning and operations. The JIOWC's commander, Maj. Gen. John C Koziol explains that his mission is to directly support STRATCOM in global deterrence, space and cyber operations through planning, coordinating and conducting information operations as well as the integrated use of operations security, military deception and electronic warfare.

http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1641&zoneid=5

The Curious China Connection

STRATEGY PAGE

07/01/2008

According to a recent analysis of malware infected websites, China houses a majority of ISPs that are connecting with malware websites. This is surprising considering the Chinese internet is very high policed by a force of 30,000 secret police technicians. Unfortunately, this means that the Chinese government most likely approves these malware sites, which vandalize websites that promote democracy in China, or protest the restrictions on Chinese internet, and there has been hacking into national websites that can be traced back to China.

http://www.strategypage.com/htmw/htiw/articles/20080701.aspx

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

CyberPro *National Security Cyberspace Institute* **P a g e | 5**
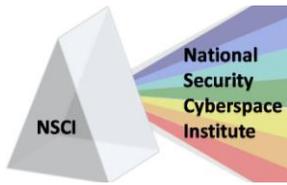
SecureWorks unmasks the Coreflood Trojan

BY: ROBERT VAMOSI, CNET NEWS
06/30/2008

SecureWorks released an analysis of the Coreflood Trojan, which started as an IRC botnet in 2002. With the help of Spamhaus, SecureWorks gained cooperation from Coreflood and found source code and 50 gigabytes of compressed data, which contained hundreds of thousands of bot IDs. The average lifecycle of each computer, from infection to removal, was 66 days. By analyzing the log files, it was determined that Coreflood would enter a network, download a copy of the installer, and then run a legitimate administration tool, which infected every computer within that domain.
http://news.cnet.com/8301-10789_3-9981248-57.html?tag=cd.blog

Mullen unsure whether stand-alone Cyber Command is needed

BY: CHRISTOPHER CASTELLI, INSIDE THE AIR FORCE
07/01/2008

Adm. Michael Mullen, the chairman of the Joint Chiefs of Staff held a question-and-answer session with military officials at the Pentagon. Mullen states that he does not know definitively about a stand-alone cyber command. Mullen said that cyber should include the military's overall involvement, and that military personnel should be careful to ensure that the proper choice of expertise is chosen and that the command could be integrated across the military.
http://www.defensenewsstand.com/defensenewsstand_spclsubj.asp?s=c4isr

Where the Bad Things Are

BY: KELLY JACKSON HIGGINS, DARK READING
06/27/2008

StopBadware.org released a report this week that states that more than half of infected websites are located on Chinese servers, six of ten network blocks that host malware are located in China, and China's infection rate is more than three times that of the world average. In addition to the StopBadware.org report, the article discusses software piracy, and how Metaforic is hoping to discourage piracy by making hacking into software so complex and time consuming that the hackers will give up.
http://www.darkreading.com/blog.asp?blog_sectionid=342&doc_id=157731&WT.svl=blogger1_1\

Pro-Russian hackers hit Lithuania

INFORMATION WARFARE MONITOR

As predicted, Russian hackers did attack Lithuania. The national communication regulator's office said that 300 websites were attacked, and their content was replaced with pictures of the Soviet Union flag and anti-Lithuanian slogans. Estonian television reported last week on appeals on Russian internet forums asking hackers to attack Lithuanian, Latvian and Estonian government websites.
http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1890&mode=thread&order=0&thold=0

Spam fighters lay down gauntlet

BBC NEWS

06/27/2008

The Messaging Anti-Abuse Working Group (MAAWG) has published new recommendations for stopping email spam. The MAAWG recommends ISPs use separate servers for receiving and forwarding emails, and blocking port 25, which is the port that transmits spam. Richard Cox, from the UK group Spamhaus says that the guidelines could be implemented within the year, however, Matt Sergeant, a senior anti-spam technologist with security form MessageLabs, believes that the new recommendations will not decrease the volume of spam by very much.
http://news.bbc.co.uk/2/hi/technology/7477899.stm

Op-Ed: Air Force works to defend cyberspace, too

BY: LT. COL. PAUL BERG

06/30/2008

Since the White House published "The National Strategy to Secure Cyberspace" in 2003, the Air Force has reorganized itself to conduct cyberspace operations and is currently building the Air Force Cyber Command, which will begin operations by October 1. Former Secretary of the Air Force Michael W. Wynne discusses how the formation of the command is a response to the growing threat of war in cyberspace and how the command is only part of the ongoing process to secure the electromagnetic environment.
http://www.afcyber.af.mil/news/story.asp?id=123104768

Israelis hack pro-Palestinian websites

BY: MOHAMMED MAR'I, ARAB NEWS

06/27/2008

A group of Israelis hacked into three Israeli-Arab and Palestinian websites, and changed the pages to a picture of the Israeli flag, the words of the Israeli anthem and pictures of Palestinian children strapped with explosives. Arabs48.com, which was hijacked, prints news on Israel in a pro-Palestinian perspective. Mahsom.com, another victim, monitors the Israeli measure on roadblocks and checkpoints in the west bank. The sites of Ezzeddine Al-Qassam Brigade, Hamas' military wing, were also hijacked.
http://www.arabnews.com/?page=4&section=0&article=111279&d=27&m=6&y=2008

Uni spies on cyber terrorism

BY: KIM WATERS, STAR NEWS GROUP

06/27/2008

Deakin University was granted a $5.9 million Federal grant to work on anti-terrorism research and development of information technology, which will be focus on the vulnerability of wireless networks. Cyber terrorism is a major concern for Australia after attacks in America and Estonia. Deakin School of Information Systems senior lecturer John Lamp states that most cyber attacks are politically motivated.
http://www.senews.com.au/story/60671

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

CyberPro   *National Security Cyberspace Institute*   **P a g e | 7**
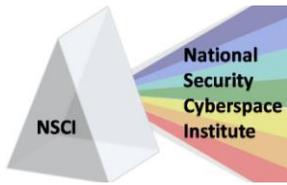
Cisco, IBM, Intel, Juniper and Microsoft fight cyber terror together

BY: TIM GREENE, NETWORK WORLD

06/27/2008

The Industry Consortium for Advancement of Security on the Internet (ICASI) is a nonprofit organization created by Cisco, IBM, Intel, Juniper and Microsoft. The organization will allow vendors and customers work together to solve global IT security threats, and develop efficient practices for responding to cyber threats. ICASI also hopes to create a forum of trust so that information can be shared freely, and so that ICASI can share information with the commercial sector.

http://www.networkworld.com/news/2008/062707-icasi-cyber-terror.html?hpg1=bn

Russian hackers planning attacks against Baltic countries and Ukraine

BY: NATHAN MCFETERS, ZDNET

06/25/2008

There is some discussion in blogs and Russian internet forums calling for Russian hackers to unite and attack websites of Latvian, Lithuanian and Estonian government institutions. Russian hackers apparently plan to replace the hijacked websites with red stars and photographs of Soviet soldiers. This would not be the first politically motivated cyber attack from Russian hackers.

http://blogs.zdnet.com/security/?p=1346

General receives nomination for Cyber Command post

BY: JOHN ANDREW PRIME, SHREVEPORT TIMES

06/25/2008

Brig. Gen Randal D. Fullhart has been nominated for a promotion to vice commander of Air Force Cyber Command at Barksdale AFB. Fullhart is currently the deputy chief of the Fort Meade based NSA's Central Security Service, and was the commandant of the Air Command and Staff College at Maxwell AFB. Fullhart holds a master's degree in national security affairs and graduated the National Security Management Course at Syracuse University and the NSA Intelligence Community Senior Leadership Program.

http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20080625/BARKSDALEWARRIOR/806250357

Uncle Sam's cyber force wants you

BY: WILLIAM ASTORE, ASIAN TIMES

06/28/2008

The United States Air Force is implementing a new vision of full-spectrum dominance, with the goal of gaining access to and control over any and all networked computers. On May 12, the Air Force Research Lab posted a request for proposals seeking contractor bids to achieve dominant cyber offensive engagement through D5, the ability to deceive, deny, disrupt, degrade and destroy enemy computer information systems.

http://www.atimes.com/atimes/Front_Page/JF28Aa01.html

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

CyberPro   *National Security Cyberspace Institute*   **Page | 8**
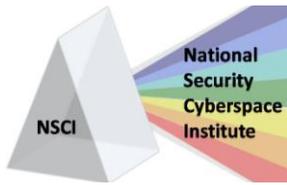
Battling the online bullies

BBC NEWS

06/27/2008

Cyber-bullying is becoming an increasing concern for parents, as children use the internet and social networking sites for bullying, including threatening or embarrassing other children and blackmail. Social networking sites connect millions of children, and Sheriff Grady Judd recommends a new system where parents log their children in using a credit card number. Other sites, like KidZui are safe and self-contained, with no messaging or chat rooms, and are a safer alternative for children.

http://news.bbc.co.uk/2/hi/programmes/click_online/7477008.stm

Satellite surveillance program dogged in approps bills

BY: BEN BAIN, FEDERAL COMPUTER WEEK

06/27/2008

The Bush administration has been trying to launch the National Applications Office that would offer satellite imagery for homeland security, emergency response and law enforcement purposes. The House and Senate Appropriations committees worry that the program would be used to spy on Americans, and will approve the program if there is a review by government auditors, and DHS submits more information.

http://www.fcw.com/online/news/152995-1.html#

GAO: DHS should merge network monitors

BY: BEN BAIN, FEDERAL COMPUTER WEEK

06/27/2008

In a report released June 26, the Government Accountability Office said that the Homeland Security Department has only completed one of three steps to establish an integrated operations center to monitor voice and data networks. The DHS has implemented common software tools for the National Coordinating Center for Telecommunications and the United States Computer Emergency Readiness Team, but has not merged the two officers or allowed private-sector critical infrastructure officials to participate at the operations center.

http://www.fcw.com/online/news/152997-1.html

Summertime security: No letup for IT

BY: ELLEN MESSMER, NETWORK WORLD

06/27/2008

This article gives an overview of IT security projects that are in the news this summer. Overstock.com will be installing a web-application firewall. The Dublin Methodist Hospital is called the "digital hospital" because of advanced wireline and wireless networks, and will be adding a biometric-based fingerprint authentication device. The University of Nevada at Reno will be adding the Mathewson-IGT Knowledge Center, which will house 400 computer workstations on a high-speed network, and books in the University library will be housed on the second floor and retrieved by a robot.

http://www.networkworld.com/news/2008/062708-user-security.html

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

CyberPro   *National Security Cyberspace Institute*   **P a g e | 9**
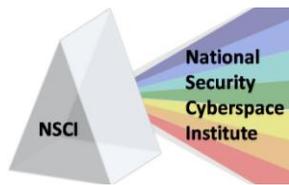
Hacker Launches Botnet Attack via P2P Software

BY: DAVID KRAVETS, WIRED BLOG NETWORK
06/27/2008

19 year old Jason Michael Milmont, agreed to plead guilty for stealing thousands of victims' personal information in a hacking scheme that originated from peer-to-peer software. Milmont controlled as many as 15,000 computers at a time, installing the Nugache Worm through installation of a peer-to-peer file sharing program. Milmont had access to the victims' personal information including credit card information, address, phone numbers and emails.
http://blog.wired.com/27bstroke6/2008/06/hacker-launches.html

Hackers hijack critical Internet organization sites

BY: GREGG KEIZER, COMPUTER WORLD
06/27/2008

A group of Turkish hackers, the "NetDevilz" claimed responsibility for hacking into the IANA and ICANN websites. Ironically, ICANN and IANA are the organizations responsible for allocating IP address space as well as managing the web's domain naming system. Visitors were redirected to a site with a defacement message. The same group of hackers broke into Photobook the week before.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9104298

Agencies hit security mark

BY: MARY MOSQUERA, FEDERAL COMPUTER WEEK
06/27/2008

With the arrival of the June 30 deadline for Trusted Internet Connections (TIC), agencies have reduced the number of external internet connections and have began to monitor the traffic that passes through the remaining nodes. Agencies now await decisions from the Office of Management and Budget regarding further gateway reduction plans. Tom Kellerman, who is the vice president of security awareness at Core Security Technologies, said that the initiatives are leaps toward a defense-in-depth strategy, but that TIC access providers should still undergo penetration testing to find new vulnerabilities.
http://www.fcw.com/online/news/153001-1.html

ICANN and IANA Sites Hacked, Redirected

BY: DAVID KRAVETS, WIRED BLOG NETWORK
06/27/2008

ICANN and IANA, both internet regulatory web sites, were hijacked and redirected to another site on Friday. The hijacking lasted for twenty minutes, and is blamed on a Turkish group called "NetDevilz." The same group hacked into Photobucket, a photo sharing site, last week.
http://blog.wired.com/27bstroke6/2008/06/icann-and-iana.html

Committees approve more money for cybersecurity

BY: BEN BAIN, FEDERAL COMPUTER WEEK
06/26/2008

Both the House and Senate Appropriations committees approved measures to fund the Homeland Security Department in 2009, and both committees granted more money to

cybersecurity than the Bush administration requested. The House measure would withhold half of the cybersecurity initiative money until the DHS submits detailed spending plans, which must be approved by the committee. The Senate also recommends that the administration conduct a privacy impact assessment of the cybersecurity initiative.
http://www.fcw.com/online/news/152976-1.html

Army hosts national youth 'cyber' science fair

BY: CARRIE MCLEROY, ARMY.MIL
06/26/2008

The Army sponsored the eCYBERMISSION competition, which brought sixteen teams of students to Washington D.C. to present science projects to a panel of judges. eCYBERMISSION is a free competition for students in the sixth to ninth grades, which encourages interest in science and engineering. The program has awarded more than $5.7 million in prize money since it began in 2002, and more than 46,000 students have participated.
http://www.army.mil/-news/2008/06/26/10380-army-hosts-national-youth-cyber-science-fair/

UK.gov calls on white hat hackers to spot data leaks

BY: CHRIS WILLIAMS, THE REGISTER
06/25/2008

UK Cabinet Secretary Gus O'Donnell introduced a new program that will target civil service systems in order to find vulnerabilities in government data handling. The program is one of many targets of scrutiny measures that will try to restore public faith in the government's efficiency in handling sensitive data. The Cabinet Office said that it will also provide reports on government progress on data handling to parliament annually.
http://www.theregister.co.uk/2008/06/25/cabinet_office_data_handling_report/

Is China Leaving the Internet's Back Door Open?

STOPBADWARE.ORG
06/24/2008

A report from stopbadware.org found that the majority of malware-infected websites, which infect visiting PCs, are located on Chinese networks. Maxim Weinstein, the manager of StopBadware.org says that the intent of the report is not to point fingers, but to open a discussion to work towards a safer internet for all users. After the publication of a similar report last year, iPowerWeb, which as home to over ten thousand infected sites, asked for help and secured their servers.
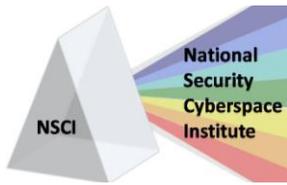http://www.stopbadware.org/home/pr_062408

Unit becomes Cyberspace Technical Center of Excellence

AIR FORCE LINK
06/25/2008

The Air Force Institute of Technology and the Center for Cyberspace Research at Wright-Patterson Air Force Base were designated as the Air Force's Cyberspace Technical Center of Excellence on June 19. The Cyberspace Technical Center of Excellence will provide cyberspace education, training, research, and technology development under the direction of the Air Force Cyberspace Education Board of Advisors. The center will also strengthen relationships between cyberspace research/education centers, Department of Defense services, federal agencies and civilian academic and commercial research organizations.
http://www.af.mil/news/story.asp?id=123104288

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

CyberPro   *National Security Cyberspace Institute*   **P a g e | 11**

AFCYBER headquarters staff to operate virtually

BY: KAREN PETITT, AIR FORCE LINK
06/24/2008

Air Force Cyber Command officials have announced that the Cyber Command headquarters will be spread out among nine locations in order to meet requirements for initial operations. No final decision has been made about the permanent location of AFCYBER, and is not expected until September 2009. Once a final base is chosen, the command may be moved completely to the chosen base, or may continue some aspects of the virtual operating environment. The article contains details on locations and proposed authorization numbers for each base.
http://www.af.mil/news/story.asp?id=123104128

Cyber Command Bill Passes Final Legislative Test

CALIFORNIA CHRONICLE
06/23/2008

The passing of SCR 117, by Senator Sam Aanestad, was passed unanimously during an Assembly Floor vote. The unanimous, bi-partisan approval of the measure means that there is unanimous support in the California State Legislature for a new military command in California. The USAF recently announced the establishment of Cyber Command, which would conduct cyber/electronic warfare and protect U.S. infrastructure networks. Cyber Command could bring thousands of private sector jobs and new businesses, which has led many states to compete to be the future location of Cyber Command headquarters.
http://www.californiachronicle.com/articles/66012

Why Overseas Hackers Are Impossible to Catch

BY: MAGGIE KOERTH-BAKER, FOX NEWS
06/23/2008

According to Congressmen Rep. Christopher H. Smith and Rep. Frank R. Wolf, Chinese hackers are responsible for breaking into Congressional computers and staling lists of Chinese dissidents and records from Congressional human rights hearings, among other information. The attacks on Smith and Wolf were traced to a computer in China, although it does not necessarily mean that computer was the source of the attack. While it is possible to trace messages across servers to the source, not every server and router saves information, and hackers will often create a fake trail.
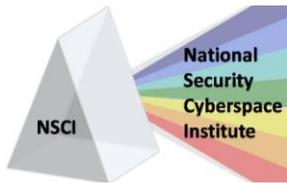http://www.foxnews.com/story/0,2933,370243,00.html?sPage=fnc/scitech/cybersecurity

Army issues Internet awareness RFP

BY: WILLIAM WELSH, DEFENSE SYSTEMS
06/24/2008

The Army has released a request for proposals for a contractor to provide Internet awareness services, including identifying implied threats, antipathy and unrest on certain domains. Contractors must provide a cyber investigator, threat analysts, and a constant watch team, and must submit weekly reports containing data and analysis. Applications are due on July 7.
http://www.defensesystems.com/news/wt/daily_news/1620-1.html

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

CyberPro   *National Security Cyberspace Institute*   **Page | 12**

Frankly Speaking: Business partners are a prime attack vector

BY: FRANK HAYES, COMPUTERWORLD

06/23/2008

The Verizon 2008 Data Breach Investigations Report is a study based on 500 cases the company was hired to investigate. According to the study, only 18% of data thefts came from the business "insiders", 78% of the data breaches would not have been stopped by fully patched systems, and 55% of the attacks did not require any special technical training. Verizon recommends implementing security measures, tightening communications with partners, and understanding business partners as potential security threats.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=320953&source=rss_topic17

China's cyber warfare against India

INDIAPOST.COM

06/23/2008

China has intensified its efforts to possess "electronic dominance" over India, with almost daily attacks on Indian computer networks. In April 2008, Indian intelligence agencies found Chinese hackers that had broken into the Ministry of External Affairs computer systems. Indian Army Chief, General Deepak Kapoor, states that the Indian army has increased security measures as well as conducting cyber-security audits.

http://indiapost.com/article/perspective/3091/

Al-Qaeda's Growing Online Offensive

BY: CRAIG WHITLOCK, WASHINGTON POST

06/24/2008

The war against terrorism has increasingly turned to television and the internet. Al-Qaeda has used new technology to communicate with loyalists and recruits worldwide, as well as release videos due to the ability to establish a secure base in tribal areas of Pakistan. Although al-Qaeda's communication operations have an internal security system that analysts say is bulletproof, which prevents the United States from disrupting communication lines or determining the location of the information.

http://www.washingtonpost.com/wp-dyn/content/article/2008/06/23/AR2008062302135.html?hpid=topnews
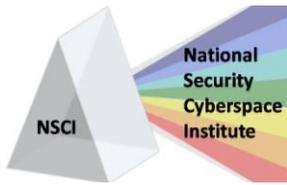
Hackers Crack London Tube's Ticketing System

BY: ALEXANDER LEW, WIRED BLOG NETWORK

06/24/2008

Dutch security researchers were able to clone the "smartcards" that London commuters use to pay transportation fares. The real threat is that the transit cards use the same Mifare chips that are in security cards, which provide access to secure locations like government offices, hospitals, and schools. Radboud University researcher Bart Jacobs, who cloned the smartcards, explains that the cards are an important national security issue, and that there are no current countermeasures.

http://blog.wired.com/cars/2008/06/hackers-crack-l.html

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

CyberPro   *National Security Cyberspace Institute*   **Page | 13**

Raytheon Awarded DARPA Contract To Increase System Information Assurance

FORBES
06/18/2008

Raytheon has been awarded a contract to test new technology for increasing system information assurance, developed by Teknowledge Corporation for DARPA. The technology will be applied to a multi-domain situational awareness system that Raytheon currently uses for defense and homeland security testing. The new technology will interpret an operator's behaviors and to determine if actions would compromise information security, and then block the harmful action.

http://www.forbes.com/prnewswire/feeds/prnewswire/2008/06/18/prnewswire200806180900PR_NEWS_USPR_____NEW003A.html

Agencies push ahead on security efforts

BY: MARY MOSQUERA, FEDERAL COMPUTER WEEK
06/23/2008

The National Institute of Standards and Technology has added updated security settings that will be installed when updating to Microsoft XP or Vista under the Federal Desktop Core Configuration (FDCC). There will not be any changes to the standard desktop view to make the security improvements faster and more efficient. The FDCC also recommends reducing the number of external internet gateways and cross-agency collaboration for sharing information and security solutions.

http://www.fcw.com/online/news/152933-1.html#

Air Force tests new broadband IT

BY: WILSON P. DIZARD III, GOVERNMENT COMPUTER NEWS
06/23/2008

The Air Force's Cyber Command recently tested Tactical Targeting Network Technology (TTNT), which is an upgraded technology for air-to-ground broadband communications. TTNT will allow aircraft the ability to transmit high-bandwidth data to ground installations and hopefully other airborne platforms. The Air Force hopes to equip all aircraft with the intelligence transmitting technology.

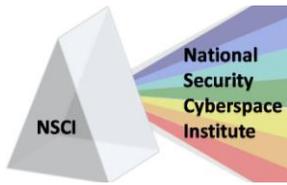http://www.gcn.com/online/vol1_no1/46529-1.html#

Cyber Security Coordination

BY: BILL UNRUE, HELP NET SECURITY
06/17/2008

In order to expedite involvement and efforts to secure cyberspace, this article recommends that government agencies and contractors should call for a cyber security summit. The goal of the summit would be to identify and prioritize security infrastructure needs, and discussing how current policies and practices are working and how they can be improved. Involvement should include federal agencies, non-profit organizations, security product manufacturers/service providers, system integrators and businesses.

http://www.net-security.org/article.php?id=1147

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

CyberPro   *National Security Cyberspace Institute*   **P a g e | 14**

A Big Pot of Money

BY: KEVIN COLEMAN, DEFENSETECH.ORG
06/30/2008

Two presidential directives aimed at defending the U.S. against cyber attacks were signed in January with an original estimated cost of $6 billion, but now are estimated to cost as much as $30 billion. Experts agree that fortifying current systems is critical and must be a high priority. The money will be spent on hardware/software, consultations, services and R&D efforts. The R&D efforts will focus on quickly developing advanced defensive capabilities, such as behavioral modeling and threat evaluations.
http://www.defensetech.org/archives/cat_cyberwarfare.html

Lauri Almann | Lessons from the cyberattacks on Estonia

BY: WYATT KASH, GOVERNMENT COMPUTER NEWS
06/16/2008

Government Computer News interviews Lauri Almann, Estonia's permanent undersecretary of Defense. Lauri Almann was part of the team that responded to the attacks on Estonia's government websites in early 2007. In the interview, Almann discusses how to guard against cyber-attacks and how Estonia is preparing for future assaults.
http://www.gcn.com/print/27_14/46457-1.html?topic=security&CMP=OTC-RSS

Former U.S. Homeland Security official warns Canada on cyber risks

BY: SHANE SCHICK, INFORMATION WARFARE MONITOR

Al Purdy, principal of DRA Enterprises, Inc. who helped to draft the United States' cyber security policy, described his frustration to the InfoSecurity Canada crowd. Purdy says, "The lack of ability to lead and take action is just shocking and unbelievable." Purdy said that there was supposed to be a shift to pro-active, risk based approach to cyber-security, but that it has not happened, and that there is a false security in the capabilities of federal agencies regarding cyber-security.
http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1853&mode=thread&order=0&thold=0
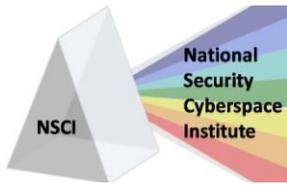
Ex-chairman of joint chiefs warns of cyber-attacks

BY: BOB COX, STAR-TELEGRAM.COM
06/13/2008

Peter Pace, retired Marine general and former chairman of the Joint Chiefs of Staff, discusses in a speech how important it is for the United States to step up efforts to anticipate and respond to cyber attacks. Pace spoke about how the U.S. dependency on computers makes us extremely vulnerable, and how an attack could be economically devastating.
http://www.star-telegram.com/business/story/696733.html

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

CyberPro   *National Security Cyberspace Institute*   **P a g e | 15**

Cyber still uncharted business realm

BY: JOHN ANDREW PRIME, SHREVEPORT TIMES

06/11/2008

State and local governments of Louisiana raised $107 million in 2007 to form the Cyber Innovation Center, in the hopes of being the future headquarters of the Air Force Cyber Command. Cyber Command, which was announced in 2006, would bring an estimated 10,000 civilian jobs. Besides Louisiana, there are 19 other states all competing for Cyber Command.
http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20080611/BARKSDALEWARRIOR/806100345

Top Secret: CIA explains its Wikipedia-like national security project

BY: HEATHER HAVENSTERIN, COMPUTERWORLD

06/10/2008

The CIA is pitching a new service called Intellipedia, which is like Wikipedia for analysts and spies. The CIA has received harsh criticism, but insists that collaboration and communication are essential to network security. The CIA hopes that Intellipedia will encourage sharing and discussion, as a community of analysts rather than a community of separate agencies.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9095638&intsrc=hm_list

Tools for the attacker, tools for the defender

BY: JOAB JACKSON, GOVERNMENT COMPUTER NEWS

06/09/2008

Intelgaurdians consultant Kevin Johnson discusses some of the tools that are used by both attackers and Web application penetration testers. The article discusses a variety of tools that can be used to test security, access and exploitation of a computer system. Most of the tools are available for free.
http://www.gcn.com/print/27_13/46438-1.html#

JCS vice chairman: break service barriers
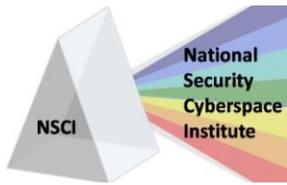
BY: CHUCK PAONE, AIR FORCE LINK

06/20/2008

Vice Chairman of the Joint Chiefs of Staff Gen. James E. Cartwright spoke at the second annual Air Force Cyberspace Symposium on June 19. Gen. Cartwright said that he thought highly of the approach that the Air Force was taking to securing cyberspace, but that the Air Force needs a more unified approach, as opposed to responding to individual issues with different groups and service organizations.
http://www.af.mil/news/story.asp?id=123103721

Air Force aims to improve electronic warfare capabilities

AIR FORCE LINK

06/20/2008

The Air Force has formed the Electronic Warfare Life Cycle Management Group to "establish a uniform approach to the research, development, and evaluation of electronic warfare hardware,

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

CyberPro   *National Security Cyberspace Institute*   **Page | 16**

software, techniques and capability." The group will find ways to more efficiently use federal funds and to eliminate the duplication of efforts and processes.
http://www.af.mil/news/story.asp?id=123103791

Senior leaders discuss need to control cyber domain, build new command
BY: ED GULICK, AIR FORCE PUBLIC AFFAIRS
06/19/2008
Both Lt. Gen. Robert J. Elder and Maj. Gen. William T. Lord gave speeches on June 18 as part of the second annual Air Force Cyberspace Symposium. Lt. Gen. Elder stressed the importance of controlling the internet and safeguarding information. Maj. Gen. Lord, who oversaw the standup of the new AFCYBER Command, discussed the mission of AFCYBER and how multiple federal organizations will work together to ensure cyber safety.
http://www.af.mil/news/story.asp?id=123103500

Secretary Wynne speaks at cyber symposium
BY: MONICA MORALES, AIR FORCE LINK
06/19/2008
Secretary of the Air Force, Michael Wynne spoke to attendees at the second Air Force Cyberspace Symposium on June 18. Secretary Wynne talked about how cyberspace will require continued efforts of Airmen and warfighters to build cyber confidence and capabilities. There have been significant advances in cyber technology, including the Air Force Cyberspace Command's publication of its strategic vision and concept of operations. Cyber capabilities have also been incorporated into Air Force exercises.
http://www.af.mil/news/story.asp?id=123103387

Ministry Of Defence to Bolster Internet Intelligence
BY: RICHARD THURSTON, SC MAGAZINE (UK)
06/13/2008
The United Kingdom Ministry of Defence is planning on expanding efforts to increase online intelligence gathering in response to the growth of international cybercrime activities. Air Commodore Graham Wright talks about the need for better risk analysis as opposed to responding to every threat possibility. Wright also emphasized the importance of information sharing and increasing the amount of publicly available information.
http://www.scmagazineuk.com/Ministry-of-Defence-to-bolster-internet-intelligence/article/111285/
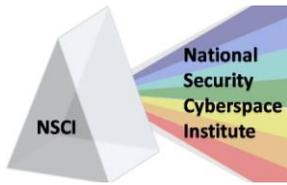
The Cyber Militia Defends America
STRATEGY PAGE
06/08/2008
The government has formed several security organizations for policing the internet. Due to a shortage of well trained workers, the government formed a "Cyber Corps" program to offer tuition assistance to college students studying information security, in order to increase the number of trained professionals. The Department of Homeland Security is working with existing computer security groups, the Department of Defense is supporting computer security operations services, and the Air Force has formed the Cyber Command, which will make the Air Force the lead organization for internet security operations.
http://www.strategypage.com/htmw/htiw/articles/20080608.aspx

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

CyberPro   *National Security Cyberspace Institute*   **Page | 17**

FISA, Finally?

BY: JED BABBIN, HUMANEVENTS.COM

06/19/2008

The Senate and House negotiators on the Foreign Intelligence Surveillance Act legislation have reached a compromise that will allow a six year renewal for the Foreign Intelligence Surveillance Act. The compromise has been in development since an interim FISA repair expired, and must be approved quickly as prior FISA court orders permitting interception of phone calls, e-mails and communications between terrorists will expire on August 3.

http://www.humanevents.com/article.php?id=27078

CyberPro Content/Distribution

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

CyberPro   *National Security Cyberspace Institute*   **P a g e | 18**