



<p>Officers</p> <p>President Larry K. McKee, Jr.</p> <p>-----</p> <p>CyberPro Research Analyst Kathryn Stephens</p>	<p><i>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.</i></p> <p><i>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 original 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.</i></p> <p><i>To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.</i></p>
--	---

Table of Contents

** CYBER-RELATED CONFERENCES **	3
*** OPEN-SOURCE MATERIAL ***	4
Sweden approves wiretapping law.....	4
Ousted Air Force secretary looks back in cyber	4
'Superhacker' Bids to Halt Extradition	4
Intel Brief: Cybercrime gets political.....	4
Study: Majority of data breaches unnoticed.....	5
50-State cyber strategy	5
Busy British Hacker Fights Extradition to U.S.....	5
How to salvage data lost to Gpcode.ak encryptor virus	5
Structural analysis of behavioral networks from the Internet	5
IBM's answer to IT skills crunch: Woo students.....	6
Wolf Reveals House Computers Compromised by Outside Source.....	6
Wolf warns lawmakers about cyberattacks	6
Task force to study IT needs of small businesses	6
Service Aims to Master Threats Before the Bad Guys	7
Lawmakers say Capitol computers hacked by Chinese	7
Special Cell Set Up To Counter Growing Threat To Space Assets	7



CyberPro

Volume 1, Edition 3
June 19, 2008

Keeping Cyber Professionals Informed

Spyware bill should focus on behavior, not technology, experts say.....	8
Security hole exposes utilities to Internet attack	8
Appropriator lists grants, cybersecurity among priorities	8
Bill aimed at small-biz cybersecurity.....	8
Analysis: Mapping malware, spam on the Web.....	9
VA promotes teamwork on cybersecurity	9
To fight future cyberbattles, Air Force recruiting part-time geeks	9
CyberPro Content/Distribution	10



**** CYBER-RELATED CONFERENCES ****

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

If you have any additions/updates/suggestions for the CYBER calendar of events, please provide them [here](#).

16-20 June 2008	Cyber Security for Process Control Systems Summer School , At the Abbey Resort on Lake Geneva, Fontana, Wisconsin, http://www.iti.uiuc.edu/events/SummerSchool2008.html
17-18 June 2008	Enterprise Security Management Spring Forum , Bellevue WA, www.afei.org
17-19 June 2008	Joint Warfighting 2008, "DoD Capabilities for the 21st Century" , Virginia Beach VA, http://www.afcea.org/events/east/08/intro.asp
17-19 June 2008	Cyberspace Symposium II , Marlborough MA, https://www.paulrevereafa.org/CyberSymposium/index.asp
23-25 June 2008	Space Warfare Symposium, "Space Situation Awareness and Command and Control: Keys to Future Global Security in Space" , Keystone, CO -- http://www.spacewarfare.org/
24-27 June 2008	Information Operations Europe 2008 , London UK http://www.asdevents.com/event.asp?ID=215
26-27 June 2008	Identity Assurance: Authentication, Protection, and Federation , Ronald Reagan International Trade Center, Washington, D.C. http://www.afcea.org/events/register.cfm?ev=17
14-17 July 2008	Annual International Test & Evaluation Association Technology Review , Crowne Plaza Hotel, Colorado Springs CO, www.itea.org
15 – 17 July 2008	Air Force Symposium 2008 – Cyberspace , Maxwell AFB (Montgomery) AL www.maxwell.af.mil/au/awc/cyberspace
25 – 26 Sept 2008	Electronic Warfare Operations and Systems 2008 , London UK, http://www.asdevents.com/event.asp?ID=241
6-8 October 2008	Strategic Space & Defense , Qwest Center Omaha Convention Center and Arena, Omaha, NE, http://www.stratspace.org/



*** OPEN-SOURCE MATERIAL ***

Sweden approves wiretapping law

BBC NEWS
06/19/2008

The Swedish government has approved a controversial new law which allows the country's intelligence bureau access to international calls, faxes and emails. There has been much heated debate over the new law, and critics say the law threatens civil liberties. Supporters of the laws say that the eavesdropping is necessary to protecting national security, and detecting attack plans using the internet and other technologies.

<http://news.bbc.co.uk/2/hi/europe/7463333.stm>

Ousted Air Force secretary looks back in cyber

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
06/19/2008

Air Force Secretary Michael Wynne spoke at Hanscom Air Force Base after being forced to resign by Defense Secretary Robert Gates. Wynne was greeted with a standing ovation at the Air Force's second Cyber Symposium, and spoke about the importance of cyberspace and information networks. Wynne has pushed the importance of information security since he took office, and he is responsible for changing the Air Force's mission statement to include cyberspace.

<http://blog.wired.com/defense/2008/06/post.html>

'Superhacker' Bids to Halt Extradition

MILITARY.COM
06/19/2008

Gary McKinnon, who is charged with hacking into 97 U.S. military computers including 16 NASA computers and one in the Pentagon, will make his plea on June 19 to stop his extradition to the United States. McKinnon is also accused of shutting down the U.S. Army's Washington network of 2000 computers for 24 hours. McKinnon states that he was not a threat to U.S. national security, as he was only looking for evidence of UFOs.

<http://www.military.com/news/article/superhacker-bids-to-halt-extradition.html>

Intel Brief: Cybercrime gets political

BY: TRAVIS SENOR, ISN
06/19/2008

According to Arbor Networks, a global network security company, claims that many of the world's cyber denial of service attacks originate in Russia and Eastern Europe, including the 2007 attack on the nation of Estonia, which brought banks, utility networks, news, and even the Prime Minister's office to a standstill. The use of botnets, which are groups of malware-infected computers, is likely to continue to increase, particularly in Russian and Eastern Europe where botnets are already used successfully for political purposes.

<http://www.isn.ethz.ch/news/sw/details.cfm?ID=19097>



Study: Majority of data breaches unnoticed

BY: JABULANI LEFFALL, GOVERNMENT COMPUTER NEWS
06/17/2008

Verizon released the 2008 Verizon Business Data Breach Investigations Report, which looked at 500 data breach cases between 2004 and 2007. Verizon found that 66% of the data breaches were caused by incompetent or weak system security. The report also states that 75% of breaches were not detected until weeks, months, or even years had passed. Surprisingly, the report also found that 90% could have been stopped by “basic” security measures.

http://www.gcn.com/online/vol1_no1/46482-1.html?topic=security&CMP=OTC-RSS#

50-State cyber strategy

BY: BOB BREWER, GOVERNMENT EXECUTIVE
06/17/2008

The Air Force Cyber Command will be spread out into cyber units located in each state. Most sites will be “network operations” but there will also be eight bases throughout the country designated as “AF Distributed Cyber Enterprise”. The location of the command’s headquarters is still unknown; 18 states have entered a sweepstakes for the headquarters. The Air Force will announce in September 2009 where the headquarters will be located.

<http://www.govexec.com/dailyfed/0608/061608wb.htm>

Busy British Hacker Fights Extradition to U.S.

BY: ALLAN HOLMES, 06/16/2008
TECHINSIDER.COM

Gary McKinnon, a 44-year old British hacker, claims to have hacked into more than 73,000 U.S. computer systems. He hacked into systems operated by both the military and NASA, and claims he was looking for evidence of extraterrestrial beings, which he believes the United States is hiding. McKinnon, who hacked under the name Solo, caused more than \$900,000 since he started hacking in 1999.

<http://techinsider.nextgov.com/>

How to salvage data lost to Gpcode.ak encryptor virus

BY: ELLEN MESSMER, NETWORK WORLD
06/16/2008

Kaspersky Lab, which first identified the GpCode.ak virus, has developed a way to recover files lost to the virus. The gpcode.ak virus encrypts files on the user’s computer and then demands a ransom to decrypt them. So far, the encryption has been too strong to crack. Kaspersky has developed a free program which can restore a copy of the lost files. Kaspersky is asking for a volunteer donation for using the PhotoRec software, but it is freely available.

<http://www.networkworld.com/news/2008/061608-kaspersky-recover-files.html?fsrc=rss-security>

Structural analysis of behavioral networks from the Internet

BY: MARK MEISS, NEWSIDENTIST.COM
06/14/2008

Mark Meiss and colleagues at Indiana University in Bloomington conducted a study on millions of online users. The team collected statistical data on emails, file sharing and browsing. They



found that there is no “normal” behavior for web users; the spread of results did not fit the standard bell curve that most statistics produce. The team hopes that their study will help to create a better idea of normal online behavior and improve information security.

<http://technology.newscientist.com/channel/tech/mg19826605.400-noone-behaves-normally-in-cyberspace.html>

IBM's answer to IT skills crunch: Woo students

BY: JOHN COX, NETWORK WORLD

06/13/2008

IBM is introducing a set of web tools and resources to help students develop valuable IT skills. IBM's Academic Initiative program has been focused mainly on working with the facilities that teach IT course, but are now shifting focus to students. The online tools and resources, including skills assessments, games and tutorials, can be integrated into college classes, and will hopefully allow students to develop IT skills that are becoming increasingly important in fast growing IT jobs.

<http://www.networkworld.com/news/2008/061308-ibm-skills.html>

Wolf Reveals House Computers Compromised by Outside Source

06/11/2008

Rep Frank Wolf introduced a resolution calling for increased security on congressional computers and information systems. Wolf spoke about computers in his personal office that were hacked into as well as computers belonging to the Foreign Affairs Committee. Wolf explains that these computers contained sensitive information as well as emails, memos, correspondence, etc. The hackers were working from inside China. Wolf gives a description of the scope of cyber attacks, and states that we are making this national security problem worse by not discussing it openly.

<http://wolf.house.gov/index.cfm?sectionid=34&parentid=6§iontree=6,34&itemid=1174>

Wolf warns lawmakers about cyberattacks

BY: WYATT KASH, GOVERNMENT COMPUTER NEWS

06/12/2008

Reps. Frank Wolf and Christopher Smith propose a resolution to better protect government computers and cell phones from cyber attacks. Wolf states that computers in his congressional office had been attacked in 2006 and 2007 by people working from inside of China, and that the hackers gained access to sensitive data. Smith states that Chinese hackers have also attacked the House Foreign Affairs subcommittee on Human Rights computer twice. Wolf explains that he feels like many government officials do not fully understand the importance of the threat of cyber attack and how to protect themselves.

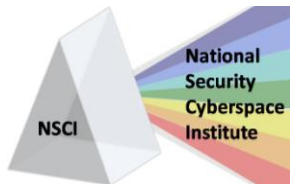
http://www.gcn.com/online/vol1_no1/46453-1.html

Task force to study IT needs of small businesses

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS

06/12/2008

Proposed bills in the House and Senate would create a Small Business Administration task force to study the IT security needs of small businesses, as well as assist small businesses in better protecting themselves. A study by the Small Business Technology Institute concluded that almost one fifth of small businesses do not have virus scanning software, 60% do not



encrypt their wireless networks and about two thirds of small businesses have no information security plan in place. The task force would provide small businesses with resources and advice to establish security plans and better protect email and internet communications.

http://www.gcn.com/online/vol1_no1/46451-1.html

Service Aims to Master Threats Before the Bad Guys

BY: RITA BOLAND, SIGNAL MAGAZINE
06/16/2008

The Air Force Research Laboratory at Wright-Patterson Air Force Base have began a 72-month effort to develop the Virtual Combat Environment for Electronic Conflict (VCEEC). VCEEC will work to identify and assess disruptive and emerging technologies that could change the future battlefield, in order to keep the U.S. on top of new capabilities and help guarantee battlefield dominance. The Air Force awarded contracts to both Northrop Grumman and Booz Allen Hamilton to develop the new virtual lab.

<http://www.afcea.org/signal/>

Lawmakers say Capitol computers hacked by Chinese

BY: PETE YOST AND LARA JAKES JORDAN, WIRED BLOG NETWORK
06/12/2008

Two congressmen announced that multiple congressional computers were hacked into by people working from inside China. Rep Frank Wolf said that four of his computers had been compromised starting in 2006, and Rep Chris Smith said that two of the computers at his global human rights subcommittee were attacked in Dec 2006 and Mar 2007. During the same time period, the House Foreign Affairs Committee was targeted at least once by someone working inside China. U.S. authorities are currently investigating whether Chinese officials copied the contents of a government laptop and then used the information to try to hack into the Commerce Department's computers. Carlos Gutierrez states that the hacking began in Aug 2006, but that he had been discouraged from disclosing the incident by government officials. The Bush administration has become "increasingly reluctant" to "discuss or acknowledge cyber attacks, especially ones traced to China."

http://hosted.ap.org/dynamic/stories/C/CHINA_HACKING?SITE=WIRE&SECTION=HOME&TEMPLATE=DEFAULT

Special Cell Set Up To Counter Growing Threat To Space Assets

SPACE WAR
06/12/2008

India's Defense Minister Shri AK Antony announced the Integrated Space Cell under the Integrated Defense Services Headquarters to respond to emerging threats to space assets. Antony also announced the Defense Information Technology Consultative Committee, a two day conference, which brings together personnel from the MoD, India's three services, Academia and industry sectors to form a common approach for the integration of information technology. Antony states that Armed Forces all over the world are becoming more technologically advanced, and explains that India must develop an integration plan, while focusing on security issues facing India.

http://www.spacewar.com/reports/Special_Cell_Set_Up_To_Counter_Growing_Threat_To_Space_Assets_999.html



Spyware bill should focus on behavior, not technology, experts say

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS

06/12/2008

Benjamin Edelman, assistant professor of business administration and spyware researcher at Harvard University, explains how any proposed anti-spyware legislation must focus on “unfair and deceptive behavior” rather than specific technology and techniques. Edelman states that narrowly defining spyware would allow criminals to adopt new techniques and avoid liability. Eileen Harrington, FTC’s deputy director of consumer protection, explains that the FTC Act’s standards of unfair and deceptive practices have been extremely resilient, and that they have brought 11 actions against spyware distributors.

http://www.gcn.com/online/vol1_no1/46447-1.html

Security hole exposes utilities to Internet attack

BY: JORDAN ROBERTSON, WIRED BLOG NETWORK

06/11/2008

Experts with Core Security Technologies discovered vulnerability in software that runs water treatment plants, natural gas pipelines and other critical utilities. Citect, which makes the CitectSCADA program, patched the hole last week, but the vulnerability could extend to other supervisory and data acquisition systems. Although there is no evidence of an attack, the discovery is a reminder that hackers could cut power to entire cities, poison water supplies or cause nuclear power plant malfunctions by attacking the utility’s controls.

http://news.wired.com/dynamic/stories/T/TEC_HACKING_UTILITIES?SITE=WIRE&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2008-06-11-07-48-41

Appropriator lists grants, cybersecurity among priorities

BY: CHRIST STROHM, CONGRESS DAILY

06/10/2008

House Homeland Security Appropriations Subcommittee chairman David Price states there will be grant funds available for cybersecurity following the mark up of the fiscal 2009 Homeland Security Appropriations bill. Price explains that cybersecurity is a high priority, although he emphasizes the importance of not letting conventional capabilities deteriorate. Price predicts the bill, which requests almost \$300 million for the cybersecurity initiative, will pass this year, but will see a fall in continuing resolutions to keep the funding going.

http://www.govexec.com/story_page.cfm?articleid=40203&dcn=e_gvet

Bill aimed at small-biz cybersecurity

BY: MARY MOSQUERA, FEDERAL COMPUTER WEEK

06/10/2008

New legislation has been introduced to help protect small businesses from hackers and information security breaches. The proposed Small Business Information Security Task Force at the Small Business Administration would help small businesses understand how to better protect themselves against information security vulnerabilities. Many small businesses currently do not have an information security plan, or even implement basic security precautions.

<http://www.fcw.com/online/news/152790-1.html>



Analysis: Mapping malware, spam on the Web

BY: SHAUN WATERMAN, SPACE WAR

06/09/2008

McAfee Inc., based in Santa Clara, California conducted the second annual "Mapping the Mal Web" report using data from an analysis of almost 10 million frequently visited websites. McAfee found that Hong Kong domain sites were the riskiest sites for internet users, with Chinese domain sites and the generic domain .info were tied for second riskiest. Finland, .fi, remained the safest domain for the second year in a row.

http://www.spacewar.com/reports/Analysis_Mapping_malware_spam_on_the_Web_999.html

VA promotes teamwork on cybersecurity

BY: MARY MOSQUERA, FEDERAL COMPUTER WEEK

06/09/2008

Representative from the Veterans Health, Veterans Benefits, National Cemetery administrations; the IT division, and Virginia's general counsel met to discuss bringing together Virginia organizations and sharing information in order to work together on information technology issues. Adair Martinez, Virginia's deputy assistant secretary for information protection and risk management explains how the department currently sends quarterly reports to Congress detailing Virginia's information security progress; they also keep an updated incident database and develop weekly reports from reported incidents. She emphasizes the importance of information sharing and improving information security "across the enterprise."

<http://www.fcw.com/online/news/152762-1.html>

To fight future cyberbattles, Air Force recruiting part-time geeks

BY: JOHN LASKER, CHRISTIAN SCIENCE MONITOR

06/06/2008

The Air Force is seeking both full and part time personnel for AFCYBER with experience in technology and will even consider hiring ex-hackers, who may have felony convictions or committed computer-related crimes. The Air Force is focusing on recruiting from the high-tech industry in hopes of building the United States defenses against cyber attacks, as well as possibly developing an offensive cyberwar plan. Richard Forno, a cybersecurity consultant in Washington, explained that the United States may have a cyberwar advantage because the U.S. has built many of the most popular software programs used globally, and may be able to exploit the software easier.

<http://features.csmonitor.com/innovation/2008/06/05/to-fight-future-cyberbattles-air-force-recruiting-part-time-geeks/>



CyberPro

Volume 1, Edition 3
June 19, 2008

Keeping Cyber Professionals Informed

CyberPro Content/Distribution

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

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 original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or the [National Security Cyberspace Institute](#).