National Security Cyberspace Institute
NSCI

# CyberPro

Volume 1, Edition 8
August 28, 2008

*Keeping Cyberspace Professionals Informed*

**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.

o

## TABLE OF CONTENTS

**Cyberspace-Related Conferences** .................................................... 4
**Cyberspace Big Picture** ............................................................. 5
Public, private sectors at odds over cyber security .................................... 5
Mutually assured destruction in cyberspace ............................................... 5
U.S. at risk of cyberattacks, experts say ................................................ 5
Cyber-attacks Gaining Acceptance as Another Weapon in War ..................................... 6
What the Georgian cyber-attacks mean for the U.S. ................................................ 6
Q&A With FBI's Cyber Division Chief ......................................................... 6
Thousands of cyber attacks each day on key utilities................................................ 6
U.S. Not Ready for Georgia-style Computer Attacks ................................................ 7
Cyberattacks on Georgian Web sites are reigniting a Washington debate ..................... 7
When Electrons Attack: Cyber-Strikes on Georgia a Wake-Up Call for Congress ............ 7
STRATCOM commander says it is time to stop playing whack-a-mole .......................... 8
Cyber chief argues for new approaches ....................................................... 8
Renuart:  New President Faces Cyber, Arctic Threats ............................................... 8
NETCOM commander weighs in on security.................................................... 8
Army CIO sets revised course ................................................................ 8
Air Force IT Conference kicks off ............................................................ 9
LandWarNet conference roundup .............................................................. 9
Army cyber ops faces forensic backlog ....................................................... 9
Sharing the Workload With Collaborative Security ................................................ 9
US Group Calls For More Electronic Warfare Investment ............................................ 9
**Cyberspace Research** ................................................................ 10
Internet-threat portal on tap from TippingPoint ............................................... 10
U.K. response team releases Net security guide ............................................... 10
New Tool Hacks the Psyche ................................................................... 10
Groups urge states to tackle more cybercrime ................................................. 11
**Georgia Cyberattack** ................................................................ 11
Lessons from Georgia.......................................................................... 11
Outside View: Georgia's cyberwar ............................................................. 11
Russia's Cyberattack on Georgia .............................................................. 11
An Army of Ones and Zeroes ................................................................... 12

Cyberspace Command ........................................................................ 12

As Russia leverages cyberspace in Georgia, Air Force Cyberspace Command is put on hold ........................................................................ 12

Air Force's Cyber Future ........................................................................ 12

Bossier leaders hold emergency Cyber Command meeting in D.C. ............................ 13

Cyberspace Hacks, Tactics and Defense ................................................. 13

Despite Airlines' Promises, Customers Find a Way to Make VOIP Calls on Flights .......... 13

The Seven Deadliest Social Networking Hacks ....................................................... 13

Latest cybersecurity threat lies in trusted software and hardware ............................. 14

Snoop software makes surveillance a cinch .......................................................... 14

Battling Botnets........................................................................................ 14

Token Security Is Just That ................................................................................ 14

KeyCzar, an open source cryptographic toolkit is released ...................................... 15

Catching The Hacking Bug ................................................................................ 15

Cyberspace – Legal ........................................................................ 15

3 takeaways from security-flaw legal flap between MBTA, MIT students ..................... 15

Gag order against MIT students dissolved by judge ............................................... 16

Judge refuses to lift gag order on MIT students in Boston subway-hack case ............... 16

AOL phisher gets seven year sentence ................................................................ 16

CyberPro Content/Distribution ................................................................ 17

## CYBERSPACE-RELATED CONFERENCES

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

| | |
|---|---|
| 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 |
| 22 Sept 2008 | **Net-Centric Operations Conference,** New Castle, N.H., http://herbb.hanscom.af.mil |
| 25-26 Sept 2008 | **Electronic Warfare Operations and Systems 2008**, London UK, http://www.asdevents.com/event.asp?ID=241 |
| 29-30 Sept 2008 | **Airbone Networks Conference,** Washington D.C., http://www.asdevents.com/event.asp?ID=267 |
| 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/ |
| 15 Oct 2008 | **Georgia Tech Information Security Center (GTISC) Emerging Cyber Security Threats Summit,** Atlanta, GA, http://www.gtisc.gatech.edu/securitysummit1008reg.html |
| 16-17 Oct 2008 | **8th Annual C4ISR Integration Conference** , Defense News Media Group, Arlington, Virginia, http://www.dnmgconferences.com/07c4isr/index.php?content=home |
| 20-21 Oct 2008 | **Space-Based Intelligence, Surveillance & Reconnaissance Conference,** Arlington, VA, http://www.asdevents.com/event.asp?ID=299 |
| 3-5 Nov 2008 | **Global MilSatCom 2008 Conference & Exhibition,** Millennium Conference Centre, London, UK, www.smi-online.co.uk/08globalmilsatcom20.asp |
| 1-3 Dec 2008 | **Defense Network Centric Operations 2008,** Arlington, VA, http://www.asdevents.com/event.asp?ID=275 |
| 14-15 May 2009 | **Electronic Warfare 2009,** London, UK, http://www.asdevents.com/event.asp?ID=302 |

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

## CYBERSPACE BIG PICTURE

### Public, private sectors at odds over cyber security

BY: JOSEPH MENN, LOS ANGELES TIMES
08/26/2008

Government officials often feel that cyberspace security would best be handled by the private sector, while the private sector feels that cybersecurity is too large of a problem to handle. The conflict between the government and the private sector is due in part to the scope of cyber security: the government oversees protection of government networks, the FBI handles cybercrime and the State Department handles international conflicts, however, the majority of the Internet's infrastructure is in the hands of the private sector. Many are calling on more action from the government to secure critical infrastructures, although both presidential candidates have barely mentioned cybersecurity.
http://www.latimes.com/business/la-fi-security26-2008aug26,0,2021258.story

### Mutually assured destruction in cyberspace

BY: VICTOR MALLET, FINANCIAL TIMES
08/20/2008

John Tkacik, senior research fellow at the Asian Studies Center of the Heritage Foundation, wrote a report earlier this year on Chinese cyber threats which listed recent security breaches and claims that the United States should be concerned over the threat of cyber attacks from China, as the U.S. and China will always be strategic enemies. The article also emphasizes that the risks of cyberwar are made greater by the absence of national guidelines and relevant international laws and treaties.
http://www.ft.com/cms/s/ca5cb050-6eb7-11dd-a80a-0000779fd18c,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2Fca5cb050-6eb7-11dd-a80a-0000779fd18c.html%3Fnclick_check%3D1&_i_referer=&nclick_check=1

### U.S. at risk of cyberattacks, experts say

BY: BRANDON GRIGGS, CNN
08/18/2008

Internet security experts predict that the United States is not prepared for cyberattacks like those aimed at Georgia recently, and claim that attacks could be devastating to the United State's economy and infrastructure.  Scott Borg, director of the United States Cyber Consequences Unit, believes that political and military conflicts will now almost always have a cyber component, and that the target of those attacks will be critical infrastructure. The largest challenge facing U.S. security experts is the difficulty in identifying the source of cyber attacks, and then the difficulty with bringing consequences to the criminals.  Some experts do, however, believe that the United States is not as vulnerable as Georgia or Estonia, who have both suffered cyber attacks recently. http://edition.cnn.com/2008/TECH/08/18/cyber.warfare/index.html

## Cyber-attacks Gaining Acceptance as Another Weapon in War

BY: BRIAN PRINCE, EWEEK.COM
08/14/3008

This article gives a brief overview of some examples of recent cyberattacks, including the attacks in Estonia, Lithuania, the breach of Pentagon e-mails, and the recent attacks against Georgia. The article emphasizes that cyberspace, specifically the Internet, is quickly becoming a powerful weapon used in terrorism and military campaigns. Don Jackson, director of threat intelligence for SecureWorks, explains that enemies will use cyberspace as much as their capability allows for cyberattacks and misinformation campaigns. http://www.eweek.com/c/a/Security/A-Year-of-CyberAttacks-Georgia-Not-First-and-Wont-be-Last-to-Fall-Victim-to-Hackers/?kc=rss

## What the Georgian cyber-attacks mean for the U.S.

BY: CYRUS FARIVAR, SALON
08/19/2008

While Georgia is receiving an onslaught of cyberattacks, some argue that the United States should be more concerned about the lack of the U.S. government's lack of knowledge of cyberspace than worry that we will suffer similar attacks. The State Department, Pentagon and private-sector experts met two months ago to discuss issues concerning cyberspace, which concluded that since no government entity has taken charge of cyberspace, nothing is getting done and that many have looked to the new administration to take charge of cyberspace. Still, the Pentagon has put a hold, and will possibly discard, the Air Force Cyber Command, which was prepared to be fully operational October 1. Many experts do agree that the United States websites aren't nearly as vulnerable as those of Georgia or Estonia, but that we still need to have some response plan in place. http://machinist.salon.com/blog/2008/08/18/georgia_cyber/index.html

## Q&A With FBI's Cyber Division Chief

BY: BRIAN KREBS, WASHINGTON POST
08/18/2008

Author Brian Krebs interviewed James Finch, the head of the FBI's Cyber Division, following the Black Hat hacker convention in Las Vegas. Finch states that he is not that concerned about internet security issues, comparing the risk of using the internet to the risk of driving a car. Finch does, however, admit that the Internet is not too difficult to crack by decrypting encryption or undermining safeguards. http://voices.washingtonpost.com/securityfix/2008/08/qa_with_fbis_cyber_crime_chief.html#more

## Thousands of cyber attacks each day on key utilities

BY: JONATHON RICHARDS, THE TIMES
08/23/2008

Lord West of Spithead, the Security Minister, states that there are thousands of attacks a day from both individuals and terrorists. British intelligence organizations have warned of threats from Russia and China, and Lord West explains that terrorist-backed hackers who attempt to break into national networks such as the National Grid's are the most serious threat.

Security experts agree that their biggest concern is from exploitation of the port of the computer system which connects to the internet.
http://www.timesonline.co.uk/tol/news/uk/crime/article4592677.ece

## U.S. Not Ready for Georgia-style Computer Attacks

BY PATRICIA RESENDE, NEWS FACTOR
08/15/2008

Security experts claim that China and Russia, both accused of cyberattacks in the past, are the biggest threat to the United States, and that the U.S. is not prepared for attacks similar to those in Georgia. Jose Nezario, a senior security researcher with Arbor Networks, explains that both Russia and China are well equipped and similar in terms of capability and programming to induce cyberattacks. Arbor Networks also claims that cyberattacks have increased in frequency and size, and that the largest attacks, those between 20GB and 40GB per second, are enough to take down any Internet service provider.
http://www.newsfactor.com/story.xhtml?story_id=0330014YR8UX

## Cyberattacks on Georgian Web sites are reigniting a Washington debate

BY: SIOBHAN GORMAN, WALL STREET JOURNAL
08/14/2008

Recent cyberattacks on Georgia are raising the question of when a cyberattack should be considered an act of war. The Georgian conflict is important because it is the first time that both cyberwarfare has been used in coordination with conventional warfare. Although U.S. officials have begun to discuss the legal and policy problems that cyberwarfare presents, experts say that the government has been slow to form a course of action for resolving these issues, despite the increasing risk of cyberattacks. Pentagon spokesman Lt. Col. Eric Butterbaugh explains that the Pentagon has no policy concerning cyberattacks as acts of war, and a meeting of intelligence agencies and private sector experts that was held two months ago concluded that because no government entity is responsible for cyberwarfare, nothing is getting done.
http://online.wsj.com/article/SB121867946115739465.html?mod=todays_us_page_one

## When Electrons Attack: Cyber-Strikes on Georgia a Wake-Up Call for Congress

BY JAMES JAY CARAFANO, PH.D., THE HERITAGE FOUNDATION
08/13/2008

According to the New York Times and others, cyberattacks on Georgia began weeks before the Russian invasion including “denial of service attacks” and other malicious acts against Georgian government computer sites. Government and business websites were intentionally disrupted during the invasion, and Russia has been accused of cyberwarfare in the past, however, the degree of involvement of the Russian government, individual hackers and organized crime groups is still unclear. The article states that the cyberattacks on Georgia should serve as a lesson for the United States, and U.S. leaders need to appoint cyber-strategic leaders as well as implement a cyber-strategy framework which includes: educating the government and private sector, making appropriate assignments and identifying valuable organizations, and accreditation to ensure that programs are successful and sustainable.
http://www.heritage.org/Research/nationalsecurity/wm2022.cfm

## STRATCOM commander says it is time to stop playing whack-a-mole

BY: SEAN GALLAGHER, DEFENSE SYSTEMS
08/25/2008

Gen. Kevin Chilton spoke at the LandWarNet conference and stated that the way the Department of Defense has been defending its networks is comparable to a game of "whack-a-mole". Chilton also said that he believes that whitelisting improve security. Chilton explained that there will be some resistance to overcome in order to get to whitelisting, especially morale issues caused from restricting non-business websites on DoD networks.
http://www.defensesystems.com/blogs/1774.html#

## Cyber chief argues for new approaches

BY: WYATT KASH, GOVERNMENT COMPUTER NEWS
08/22/2008

Air Force Gen. Kevin Chilton, the commander of U.S. Strategic Command in charge of cyberspace, spoke at the Army LandWarNet conference in Florida and explained that cyberspace should be seen as a operating domain equal to air, sea, land and space. Chilton also explained that many cyberattacks that are thought to be military threats are probably just individuals looking for information. Chilton states that he feels that the major concern with cyberspace, besides protection, is to figure out how to operate while under attack.
http://www.gcn.com/online/vol1_no1/46979-1.html?topic=security&CMP=OTC-RSS

## Renuart: New President Faces Cyber, Arctic Threats

BY: JOHN T. BENNETT, DEFENSE NEWS
08/20/2008

Air Force Gen. Victor Renuart believes that it will require the cooperation of many nations to secure cyberspace, and states that defining what is an act of war in regards to cyberattacks is a top priority, although no nation has taken action so far. A report released by the House Permanent Select Committee on Intelligence states that details of President Bush's secret, multibillion-dollar cyber security program have still not been released, and the program is still open to question. The report also states that the cyber program will require a partnership with industry that will be challenging to develop.
http://www.defensenews.com/story.php?i=3684947

## NETCOM commander weighs in on security

BY: BARRY ROSENBERG, GOVERNMENT COMPUTER NEWS
08/21/2008

Network and data security is a top priority for the modern-day Army as commanders have become network dependent, according to Brig. Gen. Susan Lawrence. Lawrence explains that the Army, Air Force, and Navy need to establish standards and protocols, information assurance, data strategy, netops, joint training and joint network management for LandWarNet, the C2 Constellation and FORCENet.
http://www.gcn.com/online/vol1_no1/46947-1.html

## Army CIO sets revised course

BY: WYATT KASH, GOVERNMENT COMPUTER NEWS
08/20/2008

Lt. Gen. Jeffrey Sorenson, the Army's chief information officer, is shifting the Army's focus to information technology operations. Sorenson has focused on four areas, which are outlined in the article, although he is still working on the 500-day plan left by Lt. Gen. Steven Boutelle. Sorenson identifies upgrading the Army's Network Service Centers and enhancing the Army's knowledge management capabilities as two of his most critical goals, stating "We're no longer net-enabled but net-dependent."

http://www.gcn.com/online/vol1_no1/46940-1.html

### Air Force IT Conference kicks off

BY: SCOTT KNUTESON, AIR FORCE LINK
08/26/2008

The Air Force Information Technology Conference began August 25 in Montgomery, AL, and features keynote speeches from Lt. Gen. Robert J. Elder Jr., the 8th Air Force commander and Robert H. Sampson, IBM's VP of Worldwide System Sales Systems and Technology Group. General Elder spoke about developing cyberspace as a warfighting domain and cyber challenges to national security. Sampson spoke about how industry partners can work with the military to understand existing capabilities as well as develop new capabilities.
http://www.af.mil/news/story.asp?id=123112474

### LandWarNet conference roundup

BY: SEAN GALLAGHER, FEDERAL COMPUTER WEEK
08/25/2008

At the recent LandWarNet conference, Lt. Gen. Jeffrey Sorenson, the Army's chief information officer, suggested that the military provide soldiers with BlackBerry-like devices that would allow them to access critical data wherever they go. The Army also announced that it will add wikis, blogs and other Web 2.0 features to the current Army Knowledge Online Web portal, which will allow users to collaborate securely on contracting issues. The Army is testing these new features, which are expected to be available for release in September.
http://www.fcw.com/online/news/153602-1.html

### Army cyber ops faces forensic backlog

BY: WYATT KASH, GOVERNMENT COMPUTER NEWS
08/20/2008

Col. Barry Hensley spoke at the 2008 LandWarNet conference in Florida, stating that there are 360 million attempted scans per day that come across the Defense Department network. Hensley explains that as the number of assaults increases, so does the challenges of forensics and attribution analysis. Hensley explained that the major issues facing cybercrime are attribution, as well as deciphering the nature of the attacks. Hensley also spoke about the changes that anti-virus vendors are making in order to improve security.
http://www.gcn.com/online/vol1_no1/46946-1.html

### Sharing the Workload With Collaborative Security

BY: JOHN H. SAWYER, DARK READING
08/13/2008

Security products are increasingly using collaborative features as opposed to a wiki, a Microsoft SharePoint server or other web-based information sharing tools. Mandiant's Intelligent Response appliance, which is designed for enterprise incident response, is a powerful tool that allows multiple incident handlers to share notes and work. Forensic software developers, Guidance Software and AccessData, also have lab editions of their software for collaboration and workload sharing. Collaborative features are becoming more popular in security products, and often allow team members to share information more easily and quickly.
http://www.darkreading.com/blog.asp?blog_sectionid=447

### US Group Calls For More Electronic Warfare Investment

BY: STEPHEN TRIMBLE, FLIGHT GLOBAL
08/04/2008

US Lawmakers Joe Pitts and Rick Larsen are leading an electronic warfare group that will work to create a senior-level post to oversee joint requirements and a dedicated career track

at all ranks, with the hope that the new objectives will be adopted by the next administration in January. Requirements and funding of Electronic Warfare programs are usually classified, which make it difficult to openly discuss concerns with current programs, however, the military and lawmakers agree that there the U.S. will soon be facing more powerful electronic threats.
http://www.flightglobal.com/articles/2008/08/04/226300/us-group-calls-for-more-electronic-warfare-investment.html

## CYBERSPACE RESEARCH

### Internet-threat portal on tap from TippingPoint

BY: TIM GREENE, NETWORK WORLD
08/19/2008

TippingPoint is testing a Web portal, ThreatLinQ, which allows customers view information gathered from intrusion-prevention systems over the last three years. Customers can view internet-threat intelligence, as well as how other customers are dealing with threats. Portal visitors can use an interactive map to find the most prevalent attacks in their areas, and TippingPoint is planning on adding a forum which will allow customers to ask other customers questions about threats.
http://www.networkworld.com/news/2008/081908-tippingpoint-internet-threat-portal.html

### U.K. response team releases Net security guide

BY: ROBERT LEMOS, SECURITY FOCUS
08/15/2008

The United Kingdom's Centre for the Protection of the National Infrastructure recently published the *Security assessment of the internet protocol*, a report which states that even the latest technical standards for building networks and networking products could still have security vulnerabilities. The report found that even the latest documentation of Internet protocols does not include solutions to the latest security problems. For example, researcher Dan Kaminsky recently discovered a way to attack the domain-name system.
http://www.securityfocus.com/brief/800

### New Tool Hacks the Psyche

BY: KELLY JACKSON HIGGINS, DARK READING
08/14/2008

Security researchers Nitesh Dhanjani and Akshay Aggarwal have been researching how online activity, especially blogging and social networking sites may give insights into user's emotions, which could be used for information gathering or as a way to influence their behavior. The researchers are building a prototype "emotion dashboard", which basically gathers information on internet users from sites like MySpace, Facebook, Twitter and blogs, and forms correlations among the user's online postings and activities, which offer insight into the user's emotions. The research

will be presented at Microsoft's Blue Hat security summit in October.
http://www.darkreading.com/document.asp?doc_id=161633

### Groups urge states to tackle more cybercrime

BY: ROBERT LEMOS, SECURITY FOCUS
08/14/2008

A report release by the Center for Democracy and Technology (CDT) and the Center for American Progress (CAP), two technology policy groups, found that most state prosecutors do not currently focus efforts on cybercrime outside of child pornography and sexual predator cases. The groups collected consumer complaints from 30 states, and found that 24 of those states had internet crime categories in their top-10 list of complaints, while four states had internet-related complaints topping the list. The report named California, Texas and Washington as states that were focusing efforts towards cybercrime, and recommended that the offices of the Attorneys General improve data collection practices.
http://www.securityfocus.com/brief/798

## GEORGIA CYBERATTACK

### Lessons from Georgia

BY: MICHAEL WYNNE, DEFENSE NEWS
08/19/2008

Because Estonian laws allow them to enter cyberwar in the defense of freedom of cyberspace, Estonia was able to send cyber warriors to Georgia to assist in stopping the cyberattacks from Russia. This article poses the question: should the United States allow American cyber warriors to assist in protecting cyberspace? The U.S. should also recognize the importance of focusing our armed forces on cyberspace education and training, to fully "exploit its leverage". Finally, our Defense Department should work to be able to offer authorities a full set of options for both offensive and defensive cyber action, before we are victims of cyberattacks similar to recent attacks in Georgia and Estonia.
http://www.defensenews.com/story.php?i=3679002

### Outside View: Georgia's cyberwar

BY: ILYA KRAMNIK, UPI
08/22/2008

Since the first day of the war, websites in Georgia and Russia have been the targets of cyberattacks, aimed at the information that the websites contained. Bringing down enemy websites is effective in blocking communication and causing confusion, which damages a rival's chance for success in a battle. Contrary to popular belief, cyberwarfare is often not more humane than traditional warfare, as attacks can paralyze important national economic and transportation systems.
http://www.upi.com/Security_Industry/2008/08/22/Outside_View_Georgias_cyberwar/UPI-54721219412152/

### Russia's Cyberattack on Georgia

BY: MALLORY FACTOR, HUMAN EVENTS
08/15/2008

As demonstrated by the recent cyberattacks on Georgia, cyberattacks are a highly effective way to cause confusion and make a country more vulnerable, especially in coordination with traditional military action. China has also used cyberspace to hack into computers in both the United States and Europe, using the intrusions for information gathering from government agencies, defense "think-tanks" and financial institutions. This year, Congress will decide the roles and missions for each of the Department of Defense services, hopefully reducing redundancies among the services and maximizing the effectiveness of each. http://www.humanevents.com/article.php?id=28044

### An Army of Ones and Zeroes

BY: EVGENY MOROZOV, SLATE
08/14/2008

Author, Evgeny Morozov writes about how simple it was to participate in the Russian cyberattacks on Georgia. Morozov explains that he set out to test whether the cyberattacks were handled as a centralized attack, and explains that he used only his laptop and internet connection to explore the cyberattacks. Morozov logged onto Russian blogs, which offered "for dummy" ways to participate in the cyber attacks. Morozov saved a copy of a Russian website to his hard drive, which allowed his browser to send thousands of queries to Georgian websites, helping to overload them. There were also how-to instructions for writing simple programs that attack websites, a website that offered URLs for websites that had not been taken down, and a software utility that allowed the user to simply enter a URL and begin a denial-of-service attack. Morozov explains that his research shows how simple it is to participate in the cyberattacks, and emphasizes that these attacks are not completely centralized but, rather, individual hackers and citizens could participate by spending only two or three minutes for set up. http://www.slate.com/id/2197514/pagenum/all/#page_start

## CYBERSPACE COMMAND

### As Russia leverages cyberspace in Georgia, Air Force Cyberspace Command is put on hold

BY: PAMELA HESS, ASSOCIATED PRESS
08/14/2008

Recent cyber headlines have focused on the Russian cyberattacks on Georgia as well as the Pentagon's delay of the Air Force's Cyberspace Command. Michael Wynne, former U.S. Air Force Secretary, states that this new form of coordinated attacks as well as the estimated 3 million daily attempted penetrations of U.S. Defense Department Networks should encourage the U.S. to make warfighting on the cyber domain a priority. A senior military commander explained to the Associated Press that delaying the Cyberspace Command does not mean that the U.S. is not addressing the threat of cyberattacks, but that the mission to defend military networks should be a part of U.S. Strategic Command, which would have responsibility for cyberspace across all services and commands. http://www.startribune.com/science/26920999.html

### Air Force's Cyber Future

BY: BOB BREWIN, GOVERNMENT EXECUTIVE
08/25/2008

New Air Force chief, Gen. Norton Schwartz is planning a reevaluation of cyberspace projects that predecessor Gen. Michael Moseley started. Lt. Col. Brad Lyons and Lt. Col. Tim Rapp of the Air Force Strategic Studies Group state that cyberspace must be a core Air Force mission, although they do see a place for joint operations in cyberspace. The Air Force has made an effort over the past year to establish itself as the "logial lead service for all things cyber". http://www.govexec.com/dailyfed/0808/082508wb.htm

**City of Hampton VA**

The City of Hampton has an advanced technology culture built on the foundation of personnel who live and work as an integral part of the community. Hampton and the surrounding region have an unmatched high technology defense industrial base and a skilled workforce with impressive education and security credentials. These critical capabilities combined with our world-class academic and government research centers, a strong pro-military culture, and superior lifestyle make Hampton the ideal choice for Cyberspace related activities. http://hamptoncyberspace.net

### Bossier leaders hold emergency Cyber Command meeting in D.C.

BY: DREW PIERSON, SHREVEPORT TIMES
08/20/2008

Bossier Parish and Bossier City officials flew to Washington, D.C. and met with staffers of federal officials from Louisiana and dozens of private companies after the announcement that Air Force leaders had halted the Cyber Command program. There were many state officials competing for their states to be the home of Cyber Command, and Bossier Parish and Bossier City had spent more than $50 million to build the Cyber Innovation Center to hopefully tip the balance in their favor. The center was developed to act as the civilian side of the military cyber presence in the area, and was expected to bring computer-oriented talent to the area.

http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=2008808200346

## Cyberspace Hacks, Tactics and Defense

### Despite Airlines' Promises, Customers Find a Way to Make VOIP Calls on Flights

BY: DAVE DEMERJIAN, WIRED BLOG NETWORK
08/25/2008

American Airlines recently announced that they will provide in-flight internet on certain routes, but that their air-to-ground system would block voice calls. Less than a week since the announcement, hackers have already found ways to use the service to accept voice-over-internet protocol calls. Calls that are set up through the networking site Twitter, involve a simple three step process that consists of logging in, adding the user name you wish to connect with and clicking on a Flash widget that appears. For now, American Airlines will try to enforce no-call policies during flights, until a solution to the issue is developed.

http://blog.wired.com/cars/2008/08/despite-airline.html

### The Seven Deadliest Social Networking Hacks

BY: KELLY JACKSON HIGGINS, DARK READING
08/26/2008

Social networking websites are rapidly becoming the next major attack venue for hackers according to security experts. These sites are particularly vulnerable because they do not always authenticate new users, and users do not usually deploy security and privacy options that are offered. Social networking sites are also effective for spreading malware quickly, as many users trust their contacts. The article also talks in detail about the "seven most lethal social networks hacks" which include impersonation, spam infections, weaponized OpenSocial applications, crossover of personal and professional online presence, XSS and CSRF attacks, identity theft, and corporate espionage.

http://www.darkreading.com/document.asp?doc_id=162226

## Latest cybersecurity threat lies in trusted software and hardware

BY: GAUTHAM NAGESH, NEXTGOV
08/25/2008

Hardware devices that make it into the wrong hands could prove to be a major security threat. Security personnel from the Executive Office of Attorneys recently found USB thumb drives that contained malicious code unattended in Justice's offices. Howard Schmidt, international president of the Information Security Forum, explains that hardware threats could come from a number of devices including digital picture frames, USB drives, hard drives and cameras. Schmidt recommends scanning external hardware before installing it on your computer and using up to date antivirus software.
http://www.nextgov.com/nextgov/ng_20080825_7185.php

## Snoop software makes surveillance a cinch

BY: LAURA MARGOTTINI, NEW SCIENTIST TECH
08/23/2008

The United Kingdom Home Office recently announced that it would make text messages, emails and internet activity details available to law-enforcement agencies, local councils and other public bodies in an effort to help security services fight crime and terrorism. In the United States, the FISA Amendments Act allows security services to intercept international phone calls and emails for up to seven days without a warrant. These and other new policies are in response to the rapid development of surveillance technologies, although the impact of these technologies has not been adequately assessed.
http://technology.newscientist.com/channel/tech/dn14591-snoop-software-makes-surveillance-a-cinch.html

## Battling Botnets

BY: PETER A. BUXBAUM, MILITARY INFORMATION TECHNOLOGY
08/20/2008

The United States military has began looking into the possibility of developing offensive and defensive botnet capabilities. Air Force Colonel Charles Willamson states the military could use excess computer capacity to develop botnet capabilities, but military botnets would not harm third party computers. Critics argue that the best defense to botnet attacks would be to layer network security, including monitoring and intrusion detection and prevention, rather than using botnets to try to counter other botnets. Network security could also be improved by blocking access to e-mails and certain websites on the Department of Defense networks.
http://www.mit-kmi.com/article.cfm?DocID=2569

## Token Security Is Just That

DARK READING
08/19/2008

Author "RSnake" gives eight reasons why implementing a token system for online activity would not work. Among these, he explains that consumers do not like carrying tokens, mostly because of the inconvenience. Tokens would

also slow down commerce; tokens would not actually solve some problems such as phishing and keystroke-logging malware; they would be very expensive to develop; there is no one authority who could be responsible for shipping and customer service; and blind consumers could not see the numbers on their tokens. RSnake emphasizes that a token system may seem like a good solution for all security problems, but they are in fact inconvenient and inefficient.
http://www.darkreading.com/document.asp?doc_id=161941&print=true

### KeyCzar, an open source cryptographic toolkit is released

SSL SHOPPER
08/18/2008

The Google security team has released Keyczar, a cryptographic toolkit which will make it "easier and safer for developers to use cryptography in their applications". Keyczar, which is extensible and cross-platform compatible, chooses safe defaults, automatically tags outputs, and provides a user-friendly and simple interface. Keyczar will not replace existing cryptographic libraries, which it is in fact built upon, but will make cryptography safer and simpler for developers to use.
http://www.sslshopper.com/article-keyczar-an-open-source-cryptographic-toolkit-is-released.html

### Catching The Hacking Bug

BY: TAYLOR BULEY, FORBES.COM
08/11/2008

Nick Harbour, a security expert from Arlington, VA, was on one of four teams that participated in the "Race to Zero" virus-writing contest at the Defcon hacker conference. The contest was sponsored by CoreTrace, an anti-virus software maker who created an obstacle course which challenged the participants to create Trojan horse viruses to beat the anti-virus software. Harbour's team took first place, finishing in six hours. After the competition, all of the viruses were run through CoreTrace's BOUNCER software, which stopped all of the viruses. Defcon reported that it notified McAfee and Symantec about the contest, but both of the two largest anti-virus software providers declined to participate.
http://www.forbes.com/technology/2008/08/11/defcon-virus-contest-tech-security-cz_tb_0811defcon.html

## Cyberspace – Legal

### 3 takeaways from security-flaw legal flap between MBTA, MIT students

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD
08/22/2008

This article presents some lessons that we can learn from the recent reversal of a gag order that blocked three MIT students from demonstrating how they found a security flaw in the ticket system of the Massachusetts Bay Transportation Authority. First, there is little agreement over what is and is not appropriate to disclose. Trying to impose gag orders on disclosures may not be a wise approach, as the court order brought more attention to the flaw. Finally, the consequences of such disclosures can be large and costly, as the MBTA will have to pay to fix security flaws as quickly as possible since the flaws have been so publicly discussed.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113284&pageNumber=1

## Gag order against MIT students dissolved by judge

BY: CHRIS KANARACUS, COMPUTERWORLD
08/19/2008

U.S. District Judge George O'Toole removed the gag order against three MIT students who had found a security flaw in the ticketing system of the Massachusetts Bay Transportation Authority. Students had planned to present their findings at the Defcon hacker convention, but were issued a ten-day restraining order after the MBA argued that exposing the vulnerability would allow criminals to damage transit operations. The Electronic Frontier Foundation, who represented the students, argued that the students had no intention of releasing key information, and that the restraining order violated the student's First Amendment rights. The lawsuit, which claims that the students violated the Computer Fraud and Abuse Act, is still open.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112968

## Judge refuses to lift gag order on MIT students in Boston subway-hack case

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD
08/14/2008

A federal judge refused to lift the temporary restraining order which prevented three MIT students from demonstrating how to hack the electronic ticketing system used by the Boston mass transit authority. The Massachusetts Bay Transportation Authority (MBTA) filed a lawsuit against the students, who had planned to release details of the vulnerability and programming code at the Defcon hacker convention. U.S. District Judge George O'Toole also required the students to submit a copy of their class paper that details the security vulnerabilities, which was requested by both the MBTA and the Electronic Frontier Foundation, a high-tech civil rights group that is representing the students in the case.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112641

## AOL phisher gets seven year sentence

BY: ROBERT MCMILLAN, COMPUTERWORLD
08/13/2008

Michael Dolan was sentenced in Connecticut federal court to seven years in prison for a phishing scheme that targeted AOL users. Dolan, who pled guilty to fraud and aggravated identity theft, received the maximum sentence according to Assistant U.S. District Attorney Edward Chang. Victims would receive e-mail messages that would infect their computers, requiring credit card and bank numbers to log on to AOL. Dolan previously served two years of probation for accessing a protected computer without authorization, and was also given nine months jail time for violating his probation.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112579

CyberPro

Volume 1, Edition 8
August 28, 2008

Keeping Cyberspace Professionals Informed

## 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.