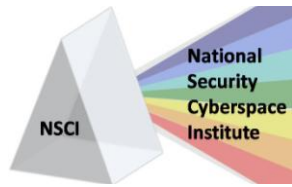




<p><b>Officers</b></p> <p>President <a href="#">Larry K. McKee, Jr.</a></p> <p>Chief Operations Officer <a href="#">Jim Ed Crouch</a></p> <p>----- CyberPro Editor in Chief <a href="#">Lindsay Trimble</a></p> <p>CyberPro Research Analyst <a href="#">Kathryn Stephens</a></p> <p><a href="#">CyberPro Archive</a></p>	<p>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.</p> <p>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 <a href="#">National Security Cyberspace Institute</a>.</p>
<p>To subscribe or unsubscribe to this newsletter click here <a href="#">CyberPro News Subscription</a>.</p> <p>Please contact <a href="#">Lindsay Trimble</a> regarding CyberPro subscription, sponsorship, and/or advertisement.</p>	

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 CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.**



## TABLE OF CONTENTS

**Table of Contents ..... 2**

**This Week in CyberPro..... 5**

**Cyber Warfare 2009: Conference brings international partners together ..... 6**

**Cyberspace – Big Picture..... 8**

    Greater Cooperation Needed to Defeat Cyber Enemies ..... 8

    Continuing the Fight Against Cyberterrorism..... 8

    Is Hacking A War Tool? ..... 8

    Threat of Cybercrime Rising ..... 8

    Cybercrime Threat Rising Sharply..... 9

    Biden Urges Cooperation on Cybersecurity ..... 9

    The Cyber Minefield..... 9

    Cyber Criminals: Digital mercenaries and Arms Dealers ..... 10

    What Happened to the Internet Jihad? ..... 10

    This Week in Magazines: Cybercrime, Financial Aristocrats and Snakes ..... 10

    GAO Finds More Security Problems in the Treasury Department ..... 10

    New Industrial Cyber Security Management Standard Published by ISA ..... 11

    Cloud Computing is a Storage Spot for Malware ..... 11

    Cybersecurity Looms as a Top Opportunity ..... 11

    Chips You Can Trust ..... 11

    Hunting Cyber-thieves ..... 12

**Cyberspace – President Obama..... 13**

    Hathaway Preps for 60-day Sprint to Obama’s Cyber-Czar Post ..... 13

    Obama Orders US Cyber security Review ..... 13

    Hathaway to head Cyber security Post ..... 13

    White House to Assume Key Role in Cyber security..... 13

    Panel Employs Full-Court Press for Cyber security ..... 14

    CRS: Chief Technology Officer Would Face Fights ..... 14

**Cyberspace – Department of Defense (DoD) ..... 15**

    Cyber Crime Conference Serves Up Reminder of What Lurks Out There..... 15

    AFOTEC Announces Mission Realignment..... 15

    Tougher Security Standards Coming for Removable Storage Devices ..... 15

    U.S. Department of Defense Putting Cloud Computing to Work..... 15

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



DoD Staff Need Help With Security .....	16
Elder: Disputes Hinder Net-centric Efforts .....	16
New Software Would Unite Defense Networks .....	16
<b>Cyberspace – Department of Homeland Security (DHS) .....</b>	<b>17</b>
DHS Wants Cyber security Sources .....	17
<b>Cyberspace – International .....</b>	<b>17</b>
NATO's Cyber Defence Warriors .....	17
Two-thirds of UK's Top IT Security Jobs Unfilled .....	17
Mangalore: Public Support Sought to Check Cyber Crimes .....	17
Report Claims German Armed Forces Setting Up Cyberwar Unit .....	18
Britain Under Attack From 20 Foreign Spy Agencies Including France and Germany .....	18
Minister: Europe Has Not Yet Done Enough on Cyber-defence .....	18
Russia Now 3 and 0 in Cyber Warfare .....	19
Russia Wields an IT Hammer .....	19
CyberBully .....	19
Are We In A Tech 'War' With Russia? .....	19
<b>Cyberspace Research .....</b>	<b>20</b>
Data Theft From Firms Topped a Trillion Dollars in 2008: Study .....	20
Microsoft SharePoint: A Weak Link in Enterprise Security? .....	20
Simulated Wi-Fi Worm Infects Thousands of Routers Overnight .....	20
Study: Airport Wi-Fi Unprotected .....	20
Putting a Price on Cyberspying .....	21
<b>Cyberspace Hacks and Attacks .....</b>	<b>21</b>
Privacy International Identifies Major Security Flaw in Google's Global Phone Tracking System .....	21
Flash Phishing .....	21
French Navy Sunk by Conficker Worm .....	21
New-age Cyber-attack Inflicts Major Damage with Modest Means .....	22
FAA Says Hackers Broke Into Agency Computers, Accessed 45,000 Names, Social Security Numbers .....	22
XSS Bug Crawls All Over PayPal Page .....	22
Hacker Breaks Into Kaspersky US Website .....	22
FBI: Cloned Debit Cards Used in Worldwide Scheme .....	23
Alleged Attacker Flaunts Details of phpBB Hack .....	23
Phishing Scam Aims to Hoodwink Hotel Habitants .....	23
The Fog of Cyberwar .....	23



Are 'Cyber-Militias' Attacking Kyrgyzstan? .....	24
DDoS Attack Boots Kyrgyzstan From Net .....	24
Cisco Warns of Four WLAN Controller Vulnerabilities .....	24
Federal Workers Notified After Virus Breach at Tech Consulting Firm .....	24
Troubled Ukrainian Host Sidelined .....	24
Less Than 10 Percent of E-mail in 2008 Was Non-malicious .....	25
Indian Embassy Web site Hack Part of Wider Assault .....	25
SQL Server Database Hack Tricks Forensics .....	25
What the Heartland Data Breach Tells Us.....	25
Heartland Sniffer Hid In Unallocated Portion of Disk.....	26
Indian Hackers Caught in Hong Kong .....	26
<b>Cyberspace Tactics and Defense .....</b>	<b>27</b>
Verizon Expands DoS Defenses in 24 Countries .....	27
Secure Your Communications Against Cyber Warfare .....	27
Metasploit Hacking Tool To Add New Services-Based Features.....	27
Coming Soon: Full-disk Encryption For All Computer Drives.....	27
Banks, Credit Unions Scramble in Wake of Heartland Breach .....	28
Securing Social Networks, from Facebook to Myspace to LinkedIn .....	28
<b>Cyberspace - Legal .....</b>	<b>29</b>
FBI Investigates \$9 Million ATM Scam .....	29
IT Worker Indicted for Setting Malware Bomb at Fannie Mae.....	29
<b>Cyberspace-Related Conferences.....</b>	<b>30</b>
<b>Employment Opportunities with NSCI.....</b>	<b>32</b>
<b>CyberPro Content/Distribution .....</b>	<b>32</b>



## THIS WEEK IN CYBERPRO

BY LINDSAY TRIMBLE, NATIONAL SECURITY CYBERSPACE INSTITUTE, INC.

There is no common definition for what makes cyber attacks evolve into cyber war or cyber terrorism. In an article from CIOL News ([page 8](#)), the author discusses recent attacks on the U.S. and French governments and the new “technology battlefield.” An article from *Strategy Page* ([page 10](#)) offers a different view of this topic, explaining that the so-called “Internet Jihad” is not as organized or as large of a threat as it appears.

These topics were discussed at an international conference I attended in London at the end of January ([page 6](#)). With representatives from 12 nations, this was a great forum for information exchange regarding cyber warfare, cyber terrorism and the new legal issues that will evolve as advances are made in technology.

In current U.S. news ([page 13](#)), Melissa Hathaway, a former consultant at Booz Allen Hamilton and top aide to President George W. Bush’s intelligence director, has been selected to lead a 60-day review of federal cyber security organization and strategy. Many predict that Hathaway will soon be appointed by President Barack Obama as the National Cyber Advisor.

Internationally, Russia is leading the headlines by being the suspected source of a distributed denial of service attack against Kyrgyzstan in January ([page 19](#)). These attacks disrupted Internet communications and have been traced back to the Russian Business Network, the group also thought to be responsible for previous attacks in Estonia and Georgia. An article from *The Guardian* ([page 23](#)) analyzes the motives behind these attacks.

Hackers are continuing to increase the scale of their attacks as well. The Federal Aviation Administration recently released a statement that hackers had broken into their administrative system, gaining access to 45,000 employees’ and retirees’ Social Security numbers and personal information ([page 22](#)). According to a Fox News article ([page 29](#)), the FBI is investigating an international ATM scam that may have resulted in the loss of more than \$9 million. The scam was just a few hours long, but hit 29 cities worldwide, including New York, Montreal, Moscow and Hong Kong.

We hope you enjoy this edition of *CyberPro*!



## **CYBER WARFARE 2009:**

### **CONFERENCE BRINGS INTERNATIONAL PARTNERS TOGETHER**

BY LINDSAY TRIMBLE, NATIONAL SECURITY CYBERSPACE INSTITUTE, INC.

With speakers from seven nations and delegates representing 12, the Cyber Warfare 2009 conference, hosted by Defence IQ, was truly an international event. Held in London Jan. 28 to 30, Cyber Warfare 2009 brought members of the military, government, academia and the private sector together with one goal – to exchange insight regarding cyber attack defense and preventative strategies.

The well-balanced line-up of speakers from the United States, United Kingdom, Estonia, Germany, Italy, Israel and Ireland provided various perspectives on what different organizations are doing in the realm of cyber defense. Each perspective demonstrated the similarities as well as the differences these nations are finding when dealing with the many realms of cyberspace. However, all came to the same conclusion: There may not be a common international definition for “cyber warfare,” but it is real and will be the next war-fighting domain. International cooperation will continue to be essential.

Speakers from U.S., United Kingdom and Italian militaries discussed the changes taking place in each of their organizations to incorporate cyberspace tactics in their missions. Training was also discussed, especially by Commander Catello Somma, who summarized Italy’s Cyber Shot 2008 exercise, their first international, inter-ministerial cyber defense exercise, held Oct. 14 to 16, 2008.

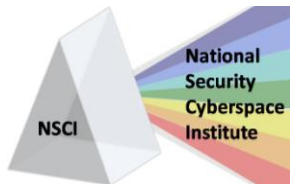
While Italy’s Cyber Shot 2008 was a defensive exercise, other militaries are preparing to take the offensive in cyberspace.

“It is far easier to attack than to defend cyberspace,” said Col. Glenn Zimmerman, U.S. Department of Defense Cyber Space Task Force.

The legal aspects and challenges of cyberspace were also discussed by members of the U.S. Air Force and NATO’s Centre of Excellence in Cooperative Cyber Defence, located in Tallinn, Estonia. Using the recent cyber attacks in Estonia and Georgia as examples, Enekin Tikk, Advisor in Public Law from the Centre of Excellence in Cooperative Cyber Defence, explained why efficient legal responses to different types of incidents need to be developed under different areas of the law.

“We should use the best practices in national and international law to achieve the goals of cyber defense strategies and policies,” Tikk said. “We need a model checklist so we know what works and why; then we can apply it to bigger or smaller countries.”

Two speakers chose to focus on cyber terrorism, explaining the motivations of terrorists and how they use technology to achieve their goals – for recruitment, the spread of propaganda or for actual cyber



attacks. Yael Shahaar, director of Israel's Database Project Institute for Counter-Terrorism, also cited possible counter-measures for cyber attacks.

According to Maj. Julian Charvat, course director for Cyber Terrorism at NATO's Centre of Excellence Defence Against Terrorism, one possible reason a "major" cyber attack has never occurred may be that terrorists are waiting until the public is so reliant on technology and cyberspace that it's not watched as closely anymore – an excellent argument for strong cyber offensive and defensive tactics to be prepared now.

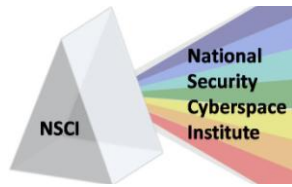
Cyber Warfare 2009's selection of speakers gave a broad overview of the ever-developing world of cyberspace, the measures that may be taken to defend against future cyber attacks and how the legal world will evolve with the evolution into a cyber-dependent world. Many see cyberspace as the next domain in war fighting. International partnerships will be imperative as this field – and cyber threats – continues to develop.

For a list of upcoming cyber-related conferences worldwide, see [page 30](#).

**NORTHROP GRUMMAN**  
DEFINING THE FUTURE™

### World-Class Cyber Solutions

- Proven, complete understanding of the entire cyber environment
- Combined experience and value of classified & unclassified domains
- Accessible, distributed world-class cyber integration capabilities
- High-performance computing centers, labs, test ranges, and R&D facilities
- Measurable, repeatable cost-effective application of technology



## CYBERSPACE – BIG PICTURE

### **Greater Cooperation Needed to Defeat Cyber Enemies**

BY: DAVID WALSH, DEFENSE SYSTEMS  
01/30/2009

Vice Adm. Carl Mauney, deputy commander for the U.S. Strategic Command, recently spoke at the Network Centric Warfare 2009 Conference in Washington, D.C. Mauney says that all elements of cyberspace operation must be integrated for the military to be able to face cyber challenges including malware, botnets, viruses and intrusions. Mauney talked about recent cyber attacks in Estonia and Georgia, and says that the United States must take action and treat cyberspace the same as other military systems. Finally, Mauney emphasized the importance of developing a clear command and control structure for cyberspace that includes cooperation between the DoD, Homeland Security and other agencies.

<http://defensesystems.com/articles/2009/01/30/cooperation-needed-to-defeat-cyber-enemies.aspx>

### **Continuing the Fight Against Cyberterrorism**

BY: ADAM DANESHEFSKY, THE SPECTRUM  
01/30/2009

The National Science Foundation (NSF) recently awarded the \$868,000 Federal Cyber Service Award to the University Of Buffalo Center Of Excellence in Information Systems Assurance Research and Education, which will go towards a scholarship for students training in Internet terrorism. The center conducts research and training to combat cyber threats that could affect the nation's critical infrastructures that are dependent upon computers such as the electric grid, telephone system and financial system. Previous projects from the center cover

topics such as real-time intrusion detection, document security, insider threat assessment and malware detection.

<http://spectrum.buffalo.edu/article.php?id=38832>

### **Is Hacking A War Tool?**

BY: DIVYA GIRISH, CIOL NEWS  
02/10/2009

The article discusses how computer hacking has no clear terms of actions and legalities, and no unified definition of what makes an online attack an act of war. The article briefly discusses attacks on White House computer networks from Chinese hackers, and attacks on the financial accounts of French President Nicolas Sarkozy. Other sites, such as the Dubai-based television channel, Al-Arabiya Television, was hacked and defaced by religious extremists. In light of these attacks, as well as countless others that are mentioned, the article states that technology is increasingly being used to build a new form of battleground as a result of attacks from increasingly political and religious motivation.

<http://www.ciol.com/News/Feature/Is-hacking-a-war-tool/10209115807/0/>

### **Threat of Cybercrime Rising**

BY: CHRISTOPHER NICKSON, DIGITAL TRENDS  
02/02/2009

A panel of experts at the recent World Economic Forum in Davos discussed cybercrime, system flaws, cyber warfare and possible solutions. The panel says that the majority of cybercrime comes from organized criminal gangs, and says that as devices become more dependent of the Internet, the risk to economies and the threat of cyber warfare also grows. One panelist also recommended the



development of an organization comparable to the World Health Organization for Internet security.

<http://news.digitaltrends.com/news-article/19112/threat-of-cybercrime-rising>

### **Cybercrime Threat Rising Sharply**

BY: TIM WEBER, BBC NEWS

01/31/2009

Experts at the World Economic Forum in Davos identified increasing threats from cyber crime, cyber warfare and design flaws in the Internet set-up. Experts also warn that as the Internet becomes "part of society's central nervous system, attacks could threaten whole economies." Experts agree that cyber crime is increasingly being carried out by well-organized criminal gangs, and say that design flaws in the set-up of the Web could have global effects if exploited. Panelists at the World Economic Forum also discussed the development of cyber warfare and the different techniques that online terrorists use to attack their enemies.

<http://news.bbc.co.uk/2/hi/business/davos/7862549.stm>

### **Biden Urges Cooperation on Cybersecurity**

BY: BEN BAIN, FEDERAL COMPUTER WEEK

02/09/2009

In a foreign policy speech at the Munich Conference on Security Policy, vice president

Joe Biden spoke about cooperating with NATO allies to address terrorism and cyber security. NATO officials announced in May the establishment of a center focused on cooperative cyber defense in Tallinn, Estonia. Estonia and Georgia were both previous targets of cyber attacks that are believed to have originated in Russia.

<http://fcw.com/Articles/2009/02/09/cyber.aspx>

### **The Cyber Minefield**

BY: SEAN GALLAGHER, DEFENSE SYSTEMS

02/09/2009

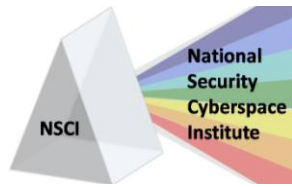
A recent attack on the Royal Air Force forced the British Ministry of Defence to shut down e-mail servers because hackers were forwarding e-mail messages to an IP address in Russia. Although cyberwarfare is the most asymmetric form of warfare, military can also use software to collect information about enemies, monitor discussions in cyberspace and attribute real-world activities. For example, voice-over-IP traffic was detected and used to trace the recent attacks in Mumbai back to Pakistan. The article explains that the United States needs to collaborate across organizational lines, and enforce information assurance policies better to combat attacks on DoD network assets.

<http://defensesystems.com/articles/2009/02/09/the-cyber-minefield.aspx>

# Raytheon

### **Raytheon**

Aspiring to be the most admired defense and aerospace systems supplier through world-class people and technology Raytheon is a technology leader specializing in defense, homeland security, and other government markets throughout the world. With a history of innovation spanning more than 80 years, Raytheon provides state-of-the-art electronics, mission systems integration, and other capabilities in the areas of sensing; effects; command, control, communications and intelligence systems, as well as a broad range of mission support services.



### **Cyber Criminals: Digital mercenaries and Arms Dealers**

BY: SEAN GALLAGHER, DEFENSE SYSTEMS  
02/09/2009

The Spamhaus Project, an international nonprofit organization that tracks spam e-mail and cyber crime, reports that the largest source of cyber crime may be the Russian Business Network (RBN), and says that the RBN hosts child pornography, malware, phishing and cyber crime. Pamela Warren, cyber crime strategist at security software vendor McAfee reports counting more than 1 million malware programs in 2008, and says that 95 percent of those programs are specifically for stealing personal information. The Defense Department is a major target of malware attacks, and recently had to issue a ban on the use of removable media to combat the spread of malicious software on the DoD's classified and unclassified networks.

<http://defensesystems.com/articles/2009/02/09/cyber-criminals-digital-mercenaries-and-arms-dealers.aspx>

### **What Happened to the Internet Jihad?**

FROM: STRATEGY PAGE  
02/08/2009

Although there have been warnings about Islamic terrorists using the Internet to launch a massive cyber attack for nearly a decade, online terrorists have had little success recruiting volunteers, and many Islamic Internet specialists have legitimate jobs in software firms and are reluctant to join in online terrorist activities. The article explains that Islamic terrorists are not nearly as organized as they appear in the media, and that the potential for attacks is real, but that the terrorist groups are not organizing and carrying out attacks.

<http://www.strategypage.com/htm/htterr/articles/20090208.aspx>

### **This Week in Magazines: Cybercrime, Financial Aristocrats and Snakes**

BY: JAMES WARREN, HUFFINGTON POST  
02/08/2009

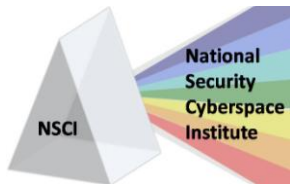
The national journal recently reported on the increase in cyber crimes including espionage and cyber warfare as part of an article called "The Cybercrime Wave." Cyber criminals are able to steal massive amounts of money from credit cards on the black market and theft of financial account information, and are increasingly attempting to steal Social Security numbers, department-store credit cards, and log-in information for social networking sites. The article explains how cyber criminals are realizing the potential of cyber crime to be more profitable and efficient than traditional crimes. The article also discusses how the Obama administration has recognized the significant damage that an organized cyber attack could do to U.S. economy and infrastructure.

[http://www.huffingtonpost.com/james-warren/ithis-week-in-magazines\\_i\\_b\\_165053.html](http://www.huffingtonpost.com/james-warren/ithis-week-in-magazines_i_b_165053.html)

### **GAO Finds More Security Problems in the Treasury Department**

BY: TIM GREENE, NETWORK WORLD  
02/04/2009

The U.S. General Accounting Office claims that lax authentication and access controls, weak encryption, insufficient firewalling and inconsistent database logging are challenges that the Financial Crimes Enforcement Network needs to address. The GAO recently released the a report, called "Further Actions Needed to Address Risks to Bank Secrecy Act Data" that says that the confidentiality and integrity of sensitive data is at risk because of these security problems. The GAO also reports that compromising sensitive information because of weak security could "undermine the ability of



the federal government, financial institutions, and law enforcement agencies to combat money laundering and terrorist financing.”

<http://www.networkworld.com/news/2009/02/0409-security-problems-treasury.html>

### **New Industrial Cyber Security Management Standard Published by ISA**

ISA.ORG  
02/05/2009

The American National Standards Institute recently approved the ASNI/ISA-99.02/01-2009, the second standard in the ISA99 series Security for Industrial Automation and Control Systems. The new standard establishes an Industrial Automation and Control Systems Security Program, explains how to set up a cyber security management system and provides guidance for compliance for each element. Further ISA99 standards that have not yet been approved include topics such as operating a security program after implementation and technical security requirements for automation and controls systems. The ISA Security Compliance Institute will identify security standards-compliant products and systems in applications in coordination with the ISA standards, and will award compliant products and systems with the ISA Secure designation. [http://www.isa.org/Template.cfm?Section=Press\\_Releases5&template=/TaggedPage/DetailDisplay.cfm&ContentID=74160](http://www.isa.org/Template.cfm?Section=Press_Releases5&template=/TaggedPage/DetailDisplay.cfm&ContentID=74160)

### **Cloud Computing is a Storage Spot for Malware**

BY: DAN RAYWOOD, SC MAGAZINE  
02/03/2009

Managing director of GSS, David Hobson, explains that hackers are able to store and transmit malicious files within cloud computing due to a method of using the Amazon EC2 Cloud Computing Service as a hosting system for BitTorrent files. Hobson warns that

companies that are thinking of using cloud computing services should seriously consider the emerging risks of cloud computing. Lew Moorman, chief strategy officer at Rackspace, argues that there are vulnerabilities, but that emerging technologies are addressing the flaws with cloud computing, and says that being unconnected is “simply not an option anymore.”

<http://www.scmagazineuk.com/Cloud-computing-is-a-storage-spot-for-malware/article/126755>

### **Cybersecurity Looms as a Top Opportunity**

BY: BILL LOOMIS, WASHINGTON TECHNOLOGY  
02/02/2009

Federal information technology and professional services industry is doing well and public federal IT and professional services firms’ stock prices continue to see gains while the market in general has experienced sharp declines. Federal IT firms will have much opportunity in cybersecurity in the next couple of years as a result of the \$10 billion cybersecurity spending that is expected over the next five years. According to the Office of the Director of National Intelligence, nondefense intelligence agency budgets will continue to grow, and funding from the national cybersecurity initiative should continue to grow during the next couple of years.

<http://washingtontechnology.com/articles/2009/02/02/loomis-cybersecurity-looms.aspx>

### **Chips You Can Trust**

FROM: STRATEGY PAGE  
01/28/2009

Because American weapons use microprocessor type chips from overseas, primarily East Asia, many are concerned that hostile nations may be using sabotaged chips in U.S. weapons. The American “Trust in Integrated Circuits” program was started four years ago, and is not yet



complete, but will develop technology and techniques for evaluating the security of chips in military equipment. There is also growing concern over the increasing sale of counterfeit computer equipment to the military.

<http://www.strategypage.com/htmw/htintel/articles/20090128.aspx>

### **Hunting Cyber-thieves**

BY: AARON NICODEMUS, WORCESTER TELEGRAM  
01/28/2009

The Open Security Foundation is a nonprofit group in Virginia that compiles information on data breaches at its Web site, [datalossdb.org](http://datalossdb.org).

The Open Security Foundation and other

companies such as the Identity Theft Resource Center and Databreaches.net publicly share information about data breaches, and attempt to find the source of data breaches and identity thefts. The organizations also lobby their states for improvements to laws on reporting data breaches. Open Security Foundation emailed information about the Heartland data breach to its e-mail list, prompting reports about the breach on media sites like NetworkWorld and the Washington Post.

<http://www.telegram.com/article/20090128/NEWS/901280477/1116>



### **CISCO**

Cisco (NASDAQ: CSCO) enables people to make powerful connections-whether in business, education, philanthropy, or creativity. Cisco hardware, software, and service offerings are used to create the Internet solutions that make networks possible-providing easy access to information anywhere, at any time. Cisco was founded in 1984 by a small group of computer scientists from Stanford University. Since the company's inception, Cisco engineers have been leaders in the development of Internet Protocol (IP)-based networking technologies.

Today, with more than 65,225 employees worldwide, this tradition of innovation continues with industry-leading products and solutions in the company's core development areas of routing and switching, as well as in advanced technologies such as: Application Networking, Data Center, Digital Media, Radio over IP, Mobility, Security, Storage Networking, TelePresence, Unified Communications, Video and Virtualization. For additional information: [www.cisco.com](http://www.cisco.com)



## CYBERSPACE – PRESIDENT OBAMA

### **Hathaway Preps for 60-day Sprint to Obama's Cyber-Czar Post**

BY: ANGELA GUNN, BETA NEWS  
02/10/2009

Melissa Hathaway, who many predict that President Obama will appoint as the National Cyber Advisor, will begin a 60-day review of federal cyber security organization and strategy that will focus on prioritizing problems that need to be addressed immediately. Hathaway previously served as a senior advisor to Mike McConnell, the former U.S. Director of National Intelligence, and she also heads the inter-agency National Cyber Study Group that recently released the Comprehensive National Cyber Initiative. Hathaway has appeared before Congress on cyber security issues more than 150 times, and formerly worked for Booz Allen Hamilton where she worked with information operations strategies and long term strategy and policy support.

[http://www.betanews.com/article/Hathaway\\_preps\\_for\\_60day\\_sprint\\_to\\_Obamas\\_cyberczar\\_post/1234259248](http://www.betanews.com/article/Hathaway_preps_for_60day_sprint_to_Obamas_cyberczar_post/1234259248)

### **Obama Orders US Cyber security Review**

BY: AGENCE FRANCE-PRESSE, ENQUIRER.NET  
02/10/2009

President Obama announced a review of U.S. cyber security this week that will aim to evaluate U.S. efforts to protect government information technology systems from security and economic threats. The 60-day review will be lead by Melissa Hathaway, a former official of George W. Bush's presidency. John Brennan, Obama's assistant for counterterrorism and homeland security, said that the national security and economic health of the United States rely on cyberspace in both the public and private sector, and that Obama is committed to

securing cyberspace while adhering to current laws and privacy rights.

<http://technology.inquirer.net/infotech/infotech/view/20090210-188443/Obama-orders-US-cybersecurity-review>

### **Hathaway to head Cyber security Post**

BY: SIOBHAN GORMAN, THE WALL STREET JOURNAL  
02/08/2009

Melissa Hathaway, a former consultant at Booz Allen Hamilton and top aide to President George W. Bush's intelligence director will head President Obama's cyber security effort according to government officials. Hathaway will conduct a 60-day review of government efforts to secure computer networks and will likely head the White House office of cyber security. Hathaway helped to develop the Bush administration's cyber security initiative, and will serve as a senior director at the National Security Council, which is actually a few rungs down from reporting directly to President Obama. Some experts are disappointed that the post wasn't higher-level.

<http://online.wsj.com/article/SB123412824916961127.html>

### **White House to Assume Key Role in Cyber security**

BY: GREGG CARLSTROM, FEDERAL TIMES  
02/03/2009

The Obama administration promised to establish a national cyber advisor who will report directly to the president and coordinate federal agency efforts and national cyber policy as part of his homeland security agenda. The position will be separate from the chief technology officer, and the White House has not announced who is being considered for the position yet. Experts explain that the advisor



will work closely with the Office of Management and Budget as well as DHS, and will need to focus on prioritization of cyber security challenges.

<http://www.federaltimes.com/index.php?S=3930494>

### **Panel Employs Full-Court Press for Cyber security**

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS  
02/09/2009

The Commission on Cyber Security for the 44<sup>th</sup> Presidency recently said that the Obama administration has made cyber security a top priority, but warns that there is much work to be done and that cyber security will be a long-term effort. Some of the panel members recommend continuing regular meetings with government officials to address emerging challenges to government information systems. Panel members hope to discuss many topics with government officials including: executive branch cyber leadership; legislation that addresses security of government systems; a review of law enforcement and investigative authorities in cyberspace; federal IT acquisition policies; international security standards; and classification of cyber initiatives.

<http://gcn.com/articles/2009/02/09/cyber-commission-full-court-press.aspx>

### **CRS: Chief Technology Officer Would Face Fights**

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK  
02/04/2009

The Congressional Research Service recently released a report that said that a federal chief technology officer would likely have to deal with “turf wars” because of uncertain and overlapping cyberspace authorities among many federal agencies. The report claims that agencies have overlapping responsibilities when it comes to innovation policy, network security and intellectual property enforcement. There is also still some uncertainty about the scope of the new position and details about where the position will be located organizationally as well as how the official will work with other agencies. Obama has previously identified some responsibilities that he would give to the new official including transparency of government operations, computer and network security, and identifying and adopting best information technology practices among federal agencies.

<http://fcw.com/articles/2009/02/04/cto-paper.aspx>

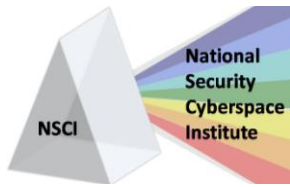


Problem. Solved.

### **High Tech Problem Solvers**

[www.gtri.gatech.edu](http://www.gtri.gatech.edu)

From accredited DoD enterprise systems to exploits for heterogeneous networks, GTRI is on the cutting edge of cyberspace technology. Transferring knowledge from research activities with the Georgia Tech Information Security Center, GTRI is able to bring together the best technologies, finding real-world solutions for complex problems facing government and industry.



## CYBERSPACE – DEPARTMENT OF DEFENSE (DoD)

### **Cyber Crime Conference Serves Up Reminder of What Lurks Out There**

BY: TIM BARKER, ST. LOUIS POST-DISPATCH

The 2009 Cyber Crime Conference sponsored by the U.S. Department of Defense targeted law enforcement agencies and included presentations by former hackers including Jeff Moss, the founder of DEF CON, and Johnny Long, with Hackers for Charity. In his presentation, Long discussed simple methods for gathering information about people and their employers. Long demonstrated how to take advantage of companies' carelessness in simple ways like finding sensitive information in dumpsters and gaining access to buildings using counterfeit ID badges. Author, Tim Barker, writes that the lesson is that hackers use both high-tech and low-tech approaches to attack companies.

<http://wiltonvillager.com/printstory/464646/>

### **AFOTEC Announces Mission Realignment**

BY: KATHERINE GANDARA, AIR FORCE LINK  
02/06/2009

The Air Force Operational Test and Evaluation Center is realigning its mission to include cyber operations, including moving 70 personnel to three AFOTEC detachments in California, Colorado and Florida. Man. Gen. Stephen T. Sargeant, AFOTEC commander, is leading the realignment efforts and emphasizes the importance of software in the command and control of modern warfare. The realignment process is estimated to take 18 months and will transfer personnel capabilities and expertise to "support existing and projected operational test and evaluation requirements."

<http://www.af.mil/news/story.asp?id=123134435>

### **Tougher Security Standards Coming for Removable Storage Devices**

BY: JILL R. AITORO, NEXTGOV.COM  
01/29/2009

The Defense Department has recently confirmed that a federal interagency that handles data encryption policies and acquisition efforts is looking into making improvements to existing technology contracts that would include stricter security standards for removable storage devices. Dave Hollis, director of cyberspace programs for Defense's Information Assurance Program, explained that the contracts that agencies use to buy software could include anti-malware protection requirements in the future. The Department recently formed the Data-at-Rest Tiger Team to implement policies on protecting sensitive information on mobile devices and removable storage, and the team is currently evaluating contract modifications that include anti-malware capabilities and encryption technical requirements.

[http://www.nextgov.com/nextgov/ng\\_20090129\\_9364.php](http://www.nextgov.com/nextgov/ng_20090129_9364.php)

### **U.S. Department of Defense Putting Cloud Computing to Work**

BY: NICOLE SCHEPKER, CLOUD COMPUTING  
JOURNAL  
02/05/2009

Chief information officer and Director of Strategic Planning for the Department of Defense, John Garing, is developing his own U.S. government cloud that can be shared among federal agencies according to a report from InfoTech. Garing support cloud computing and says that the government should pay for only the computing power that it uses and needs. Garing also says that cloud computing would allow companies to free up their customers



from having to pay for their own hardware and facilities, and says that he was inspired by sites like Amazon.com and Salesforce.com when developing his cloud.

<http://cloudcomputing.system.com/node/832419>

### **DoD Staff Need Help With Security**

BY: AHARON ETENGOFF, IT EXAMINER  
02/02/2009

The Department of Defense is currently offering free corporate editions of Symantec and McAfee anti-virus software for home use for service members and department employees in an effort to improve network security. Staff Sergeant Luis Nunez explains that recent worms such as the Downadup or Conficker worm are spreading rapidly through networks, and many experts fear that the worm may be hiding an advanced malicious program which could be woken up at any time. Chief technical officer of Mirage Networks, Grant Hartline, says that the worm may be a distraction to hide harmful malware, and is lying dormant until some trigger unleashes the worm's full potential.

<http://www.itexaminer.com/dod-staff-need-help-with-security.aspx>

### **Elder: Disputes Hinder Net-centric Efforts**

BY: DAVID WALSH, DEFENSE SYSTEMS  
01/30/2009

Air Force Lt. Gen. Robert Elder recently spoke at the Network Centric Warfare 2009 Conference, and said that disputes between cyber professionals over managing the structure is often a challenge to improving cyber security. Elder explains that there are three bureaucracies fighting to control cyberspace: the communications community, which focuses

on how the Defense Department establishes networks and IP-based systems; the intelligence community, which believes that DoD controls could make information gathering more difficult; and the operational community which Elder believes should control cyberwar capabilities. Elder said that professionals are focusing too much on the systems themselves and not enough on the bigger picture of why the systems need to be secured.

<http://defensesystems.com/articles/2009/01/30/disputes-hinder-net-centric-efforts.aspx>

### **New Software Would Unite Defense Networks**

BY: SHAUN WATERMAN, WASHINGTON TIMES  
01/29/2009

New software is being tested by U.S. Central Command that would allow military computers to connect to both classified and unclassified networks at the same time. Elwood Jones, a program manager at CENTCOM, reports that CENTCOM has engaged in a testing process called a Joint Capabilities Technology Demonstration Project called "One Box, One Wire" or OB1, and plans to release the software within three years. The new software is being developed by Integrity Global Security, and their executive vice president, Michael Liacko, explains that CENTCOM currently uses 14 different computer networks that must have physically separate connections, wires and computers.

<http://www.washingtontimes.com/news/2009/jan/29/revolutionary-software-to-unite-defense-networks/>



## CYBERSPACE – DEPARTMENT OF HOMELAND SECURITY (DHS)

### DHS Wants Cyber security Sources

BY: BEN BAIN, FEDERAL COMPUTER WEEK  
02/09/2009

The Homeland Security Department is looking into which contractors could assist DHS with cyber security projects, specifically contractors that could provide support to its National Cyber Security Division. The NCDS currently runs the United States Computer Emergency Readiness

Team. DHS is looking into industry's ability to provide systems engineering, management of cyber protection technical programs, technical coordination between DHS offices and security architecture and analysis support.

<http://fcw.com/articles/2009/02/09/ncsd.aspx>

## CYBERSPACE – INTERNATIONAL

### NATO's Cyber Defence Warriors

BY: FRANK GARDNER, BBC NEWS  
02/03/2009

NATO reports that their computers are constantly under attack from hackers despite the creation of a cyber defense policy and response team that was established after the 2007 cyber attacks on NATO member Estonia and recent attacks in Georgia. Turkish IT expert Suleyman Anil explains that hackers gather information about NATO officials and then send e-mails that could infect the victim's machine with a Trojan or worm. NATO also says that the greatest threat that they face is a hacker changing data without being detected.

<http://news.bbc.co.uk/2/hi/europe/7851292.stm>

accreditation in the security field to provide professionals with training and monitoring. Sharon Wiltshire, chairman of the Infosec Training Paths & Competencies program, says that more people completing the accreditation will help meet the UK demand for computer security staff, and benefit organizations that employ security professionals.

<http://www.silicon.com/research/specialreport/s/future-proofing/two-thirds-of-uks-top-it-security-jobs-unfilled-39383815.htm>

### Two-thirds of UK's Top IT Security Jobs Unfilled

BY: NICK HEATH, SILICON.COM  
02/03/2009

Paul Dorey, chairman of the Institute of Information Security Professionals, explains that only one-third of vacant chief security officer positions in the UK have been filled in the past four months, due to a shortage of IT skills. Dorey says that employers are all after the same people and that there needs to be more

### Mangalore: Public Support Sought to Check Cyber Crimes

FROM: MANGALOREAN  
02/03/2009

Additional Superintendent of Police R. Dileep calls for public cooperation in the enforcement of cyber laws because of the increase of cyber crime and warfare. Dileep requests that the public educate themselves on modern technologies and cyber crimes, and warns users against giving out personal information online. KILPAR Chairman G Dakshinamurthy says that the confusion regarding current cyber laws needs to be addressed before developing amendments or new legislations.

<http://mangalorean.com/news.php?newstype=local&newsid=111232>



### **Report Claims German Armed Forces Setting Up Cyberwar Unit**

FROM: HEISE ONLINE  
02/09/2009

According to Spiegel magazine, German armed forces are setting up a cyberwar unit that will work to protect the German IT infrastructure as well as carry out reconnaissance missions and interventions on enemy networks. The unit is reportedly assigned to Strategic Reconnaissance Command and is being headed by Brig. Gen. Friedrich Wilhelm Kriesel. The unit will include dozens of IT graduates from the two Universities of the Armed Forces and will be stationed in Rheinbach.

<http://www.heise-online.co.uk/news/Report-claims-German-armed-forces-setting-up-cyberwar-unit--/112595>

### **Britain Under Attack From 20 Foreign Spy Agencies Including France and Germany**

BY: SEAN RAYMENT, TELEGRAPH.CO.UK  
02/08/2009

A government security document that was obtained by the UK's Sunday Telegraph found that Britain is a high priority espionage target, and said that Iran, Syria, North Korea and Serbia as well as members of the European Union were operating within the UK. The report warns against focusing solely on attacks from al

Qaeda, and says that foreign spies are attempting to steal military, communications, genetics and aviation secrets. The report estimates that 20 foreign intelligence services are working to steal UK secrets, and identifies Russia and China as the most concerning threats.

<http://www.telegraph.co.uk/news/newsttopics/politics/defence/4548753/Britain-under-attack-from-20-foreign-spy-agencies-including-France-and-Germany.html>

### **Minister: Europe Has Not Yet Done Enough on Cyber-defence**

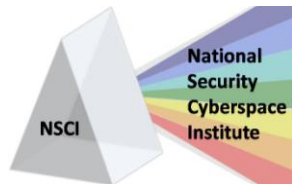
FROM: MONSTERS AND CRITICS.COM  
02/04/2009

Estonian Defence Minister Jaak Aaviksoo said that there has not been enough done to protect European Internet and communication systems from cyber attacks. Aaviksoo has been a leader of cyber defense since the Russian cyber attacks on Estonian government networks in 2007. Aaviksoo says that the European Union has not reacted to the attacks with adequate coordination, and that the group must unite efforts of various national defense and law enforcement agencies especially with countries that are a safe haven for cyber criminals.

[http://www.monstersandcritics.com/tech/news/article\\_1457522.php/Minister%AOEurope\\_has\\_not\\_yet\\_done\\_enough\\_on\\_cyber-defenc](http://www.monstersandcritics.com/tech/news/article_1457522.php/Minister%AOEurope_has_not_yet_done_enough_on_cyber-defenc)



Alion is a progressive employee-owned research, management and technology company with worldwide government and commercial capabilities supporting complex programs including network and information security, M&S, experimentation, testing and Risk / Vulnerability tools.



### **Russia Now 3 and 0 in Cyber Warfare**

BY: KEVIN COLEMAN, DEFENSE TECH  
02/02/2009

Russia launched a distributed denial of service attack against Kyrgyzstan in January 2009 which disrupted Internet communications in the country that has been traced back to the Russian Business Network (RBN) which is also thought to be responsible for previous attacks against Estonia and Georgia. Many experts believe that the Russian government may have supported or hired the hackers to carry out the attacks. Cyber Intelligence Analysts explain that the attacks aimed to disrupt demands to prohibit access to a U.S. military airbase in Afghanistan, and that Russian officials want the base closed as soon as possible.  
<http://www.defensetech.org/archives/004667.html>

### **Russia Wields an IT Hammer**

BY: DARLEEN HARTLEY, IT EXAMINER  
01/30/2009

A recent report from research firm RNCOS found that outsourcing is the fastest growing segment of Russia's IT industry, and the Russian government is expanding the nation's IT infrastructure and developing its IT and outsourcing industry. Private sector investments in Russia from both domestic and international companies are also paying for new and expanded software development centers. The article claims that Russia has more qualified software professionals with advanced technical skills than even India or China, and Russia now holds 50 percent of the offshore outsourcing in Eastern Europe.  
<http://www.itexaminer.com/russia-wields-an-it-hammer.aspx>

### **CyberBully**

STRATEGY PAGE  
02/01/2009

Russian computer hackers recently shut down Internet service in Kyrgyzstan because of the

country's resistance to Russian attempts to control Kyrgyzstan's oil and natural gas fields. Russia has previously attacked Estonia and Georgia when they had offended the Russian government. In all of these attacks, Russian hackers used botnets that included zombie computers on Russian government networks, to launch distributed denial of service attacks on enemy networks. Although Estonia called on NATO to address cyber warfare after the Russian attacks in 2007, NATO never took any action against Russia. Because there have not previously been consequences for cyber attacks, Russia is using their cyber capabilities to bully and intimidate its neighboring countries.

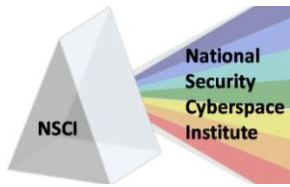
<http://www.strategypage.com/htmw/htiw/articles/20090201.aspx>

### **Are We In A Tech 'War' With Russia?**

BY: ROB ENDERLE, DARK READING  
01/29/2009

Author Rob Enderle claims that Eastern European botnets and attacks, specifically those originating in Russia, are likely government-backed, and argues that the government support of hacking tools is a form of tech war. At the World Economic Crisis, Putin criticized Dell, belittling their business and claiming that Russian software was superior. Enderle says that Putin was criticizing Western technology, and implying that there was an electronic war between the U.S. and Russia. Enderle also writes that the Russian cyberassault that took Kyrgyzstan offline may have been a sort of weapons test for Russian hackers.

[http://www.darkreading.com/blog/archives/2009/01/are\\_we\\_in\\_a\\_tec.html;jsessionid=KEHIIU3DCDU1UQSNLDLOSKHSCJUNN2JVN](http://www.darkreading.com/blog/archives/2009/01/are_we_in_a_tec.html;jsessionid=KEHIIU3DCDU1UQSNLDLOSKHSCJUNN2JVN)



## CYBERSPACE RESEARCH

### **Data Theft From Firms Topped a Trillion Dollars in 2008: Study**

SPACEWAR  
01/30/2009

Security firm McAfee recently presented research that found that global losses from data theft came to more than a trillion dollars in 2008. McAfee chief executive Dave DeWalt explains that the findings include information from more than 800 CIO's from Japan, China, India, Brazil, Britain, Dubai, Germany and the U.S. Experts warn that the current economic crisis is forcing firms to cut costs, resulting in weakened computer security practices. The study also found that there is an increasing risk of insider threats as job seekers or frustrated employees may steal information, and identified China, Pakistan and Russia as hot spots for data theft.

[http://www.spacewar.com/reports/Data\\_theft\\_from\\_firms\\_topped\\_a\\_trillion\\_dollars\\_in\\_2008\\_study\\_999.html](http://www.spacewar.com/reports/Data_theft_from_firms_topped_a_trillion_dollars_in_2008_study_999.html)

### **Microsoft SharePoint: A Weak Link in Enterprise Security?**

BY: TIM WILSON, DARK READING  
01/28/2009

A recent study from Osterman Research found that only 60 percent of companies have security tools specifically for Microsoft's SharePoint, and President Michael Osterman explains that SharePoint data tends to go require more than traditional server and endpoint security applications because of sharing across networks and applications. Another study by Courion, a SharePoint security provider, found that 25 percent of IT managers felt that their SharePoint security as weak and that nine percent of the respondents reported that their organizations had suffered a data breach because of a leak of data from SharePoint.

<http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=212903345>

### **Simulated Wi-Fi Worm Infects Thousands of Routers Overnight**

BY: TIM WILSON, DARK READING  
01/28/2009

Researchers at the Indiana University in Bloomington recently released conducted simulated malware attacks on Wi-Fi networks in seven U.S. cities that were able to spread to thousands of Wi-Fi routers overnight. A simulated attack in New York was able to infect more than 18,000 routers in two weeks. Steven Myers, assistant professor at Indiana University's School of Informatics, said that an infected router could monitor PC's Internet connections and send information back to the worm's creators. The worm could also search data streams for credit card information.

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212903193>

### **Study: Airport Wi-Fi Unprotected**

BY: BRAD GOODE, KING 5 NEWS  
01/27/2009

Wireless security firm AirTight Networks recently sent hackers to 20 U.S. airports, and found that Wi-Fi users in the airports could be hacked and spied on. Once the hackers break into a system, they are able to see passwords and files from the victims. AirTight recommends looking into the security measures that hotspot networks offer. The article also includes a best practices checklist of security suggestions for Wi-Fi networks including removing peer-to-peer networks, connecting only to trusted networks, using a VPN client when connecting over public Wi-Fi spots, and avoiding confidential or



sensitive information over unencrypted connections.

[http://www.nwcn.com/sharedcontent/northwest/travel/stories/NW\\_012709WAK-seatac-airport-wifi-ks.c1adfbf.html](http://www.nwcn.com/sharedcontent/northwest/travel/stories/NW_012709WAK-seatac-airport-wifi-ks.c1adfbf.html)

### **Putting a Price on Cyberspying**

BY: BRIAN KREBS, WASHINGTON POST  
01/26/2009

A recent study by Purdue's Krannert School of Management and McAfee found that breaches in research and development secrets last year resulted in \$4.6 million in lost or stolen intellectual property per company. While

companies are required to disclose details of data leaks of customer or employee data, other types of data loss including research and development or other strategic data are still rarely reported. Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit, says that this data leakage could undermine the national economy by giving other countries and companies that steal information an advantage. [http://voices.washingtonpost.com/securityfix/2009/01/does\\_profit\\_trump\\_nationalism.html?wprss=securityfix](http://voices.washingtonpost.com/securityfix/2009/01/does_profit_trump_nationalism.html?wprss=securityfix)

## CYBERSPACE HACKS AND ATTACKS

### **Privacy International Identifies Major Security Flaw in Google's Global Phone Tracking System**

PRIVACY INTERNATIONAL  
02/05/2009

One day after Google introduced its "Latitude" phone tracking system, Privacy International reports that the Google system lacks sufficient safeguards to protect its users from breaches of the tracking technology. Before a person can be tracked by the service, there must be a sharing arrangement with a requesting party, after which location data is made available on a continuous basis. Privacy International claims that the potential for privacy breaches if a second party gains physical access to a user's phone and enables Latitude without the user's knowledge or consent. Privacy International writes that only some mobile devices receive prompts that the service has been enacted, so users could be on enabled phones without ever knowing.

<http://www.privacyinternational.org/article.shtml?cmd%5b347%5d=x-347-563567>

### **Flash Phishing**

BY: SAI NARAYAN NAMBIAR, SYMANTEC  
01/30/2009

Several phishing Web sites are beginning to use Flash-based content instead of traditional HTML to avoid detection by tools that analyze page content. Hackers recreate front pages of legitimate Web site and then trick users into clicking malicious links that launch a Flash applet. The attackers are then able to inject the victims' machine with malicious code that send the victims' authentication cookies to the attackers. Flash phishing attacks require the victim to have an installed Flash player, although machines without the Flash player are redirected to a download site that installs the Flash player.

[https://forums.symantec.com/t5/blogs/blogarticlpage/blog-id/online\\_fraud/article-id/104](https://forums.symantec.com/t5/blogs/blogarticlpage/blog-id/online_fraud/article-id/104)

### **French Navy Sunk by Conficker Worm**

BY: ROBERT MCMILLAN, TECHWORLD  
02/10/2009

The French navy recently came under attacks from the massive Conficker worm, and was



forced to shut down network connectivity in an effort to stop the spread of the worm over its Intramar network. Web browsing and email messaging were disrupted as part of the efforts to contain the infection. Reports claim that the worm was introduced to the system by an infected USB drive, although the worm can copy itself to other PCs once one machine is infected. The worm spread through a local area network, although firewall software is effective in stopping the worm.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=110624>

### **New-age Cyber-attack Inflicts Major Damage with Modest Means**

BY: DAN GOODIN, THE REGISTER  
02/10/2009

A new cyber attack technique that tricks servers into overloading victims with more information than they can handle is becoming increasingly common and will likely be added to commercial attack kits soon, according to Don Jackson, a researcher with SecureWorks. Attackers have targeted pornography sites so far, and preventing the attacks will require changes to each vulnerable DNS server on the Internet. The attacks that Jackson has observed often accompany traditional distributed denial of service attacks, and he claims the technique will soon be included in DDoS packages.

[http://www.theregister.co.uk/2009/02/10/new\\_dns\\_amplification\\_attacks/](http://www.theregister.co.uk/2009/02/10/new_dns_amplification_attacks/)

### **FAA Says Hackers Broke Into Agency Computers, Accessed 45,000 Names, Social Security Numbers**

BY: JOAN LOWY, STAR TRIBUNE  
02/09/2009

The Federal Aviation Administration recently released a statement that said that hackers had broken into the Administration's computer system, and had gained access to names and Social Security numbers of 45,000 employees

and retirees. Tom Waters, president of American Federation of State, County and Municipal Employees Local 3290, also reported that a second breach at the Administration compromised personal information including encrypted medical information. The attacks have been turned over to law enforcement agencies, and affected employees are being notified of the breach.

<http://www.startribune.com/nation/39336392.html>

### **XSS Bug Crawls All Over PayPal Page**

BY: DAN GOODIN, THE REGISTER  
02/10/2009

Online payment site PayPal has been targeted again by a cross-site scripting bug that hackers could use to obtain user passwords or steal authentication cookies. The attack has affected users of Internet Explorer and Firefox, although the Firefox NoScript plug-in did successfully block the infected page from loading. XSS bugs use manipulated URLs to spread unauthorized code or content, and are able to bypass the policy that keeps cookies from one domain from being accessed at a different address.

[http://www.theregister.co.uk/2009/02/10/pay\\_pay\\_xss\\_bug/](http://www.theregister.co.uk/2009/02/10/pay_pay_xss_bug/)

### **Hacker Breaks Into Kaspersky US Website**

BY: JOHN E. DUNN, TECHWORLD  
02/09/2009

A hacker recently broke into the Web site of Kaspersky Lab, and publicized table names from the company's U.S. sales database. The hacker defaced the sites and gained access to confidential customer and company information. The attack is believed to be an SWL injection attack, and the attacker said that he would not post screenshots with confidential personal information or codes, which leads experts to believe the hacker was not attempting to steal money from the attack.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=110604>



### **FBI: Cloned Debit Cards Used in Worldwide Scheme**

BY: ELINOR MILLS, CNET  
02/05/2009

The FBI in Chicago recently released surveillance footage of two suspects at ATMs that may be involved in a worldwide scam that uses cards created by hackers to withdraw money from compromised accounts. Hackers breached the records of RBS WorldPay, an Atlanta company that processes financial transactions, and the criminals have reportedly been able to withdraw as much as \$9 million so far. The RBS WorldPay breach compromised information from as many as 1.5 million cardholders including 1.1 million Social Security numbers.

[http://news.cnet.com/8301-1009\\_3-10158062-83.html](http://news.cnet.com/8301-1009_3-10158062-83.html)

### **Alleged Attacker Flaunts Details of phpBB Hack**

SECURITY FOCUS  
02/05/2009

A hacker that was able to exploit a vulnerability in the PHPlist newsletter manager and access critical files on phpBB.com, posted detailed information about how he hacked into the site on a Blogger. The security flaw was not patched until two weeks after the attacks, and administrators of phpBB.com said that the attacker was able to gain entry to the site and copy a complete backup of all of the emails on file. The phpBB group suggests that members of the list that was breached change their passwords on other Web sites and took the site offline for maintenance.

<http://www.securityfocus.com/brief/902>

### **Phishing Scam Aims to Hoodwink Hotel Habitants**

BY: JOHN LEYDEN, THE REGISTER  
02/05/2009

Security community FraudTip.com warns that more than 71,000 travelers that use sites of hotel chains including Hyatt, Comfort Inn, Ramada, Days Inn, and Wyndham have been redirected to counterfeit sites. The attack uses advertising, third-party reservation systems and Internet browser crimeware to send visitors to fake versions of hotel chain websites. Roger Thompson, chief of research at AVG, explains that the attacks have all the characteristics of traditional phishing assaults, although these types of attacks usually target banks or ecommerce sites.

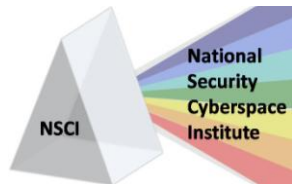
[http://www.theregister.co.uk/2009/02/05/hotel\\_phishing\\_scam/](http://www.theregister.co.uk/2009/02/05/hotel_phishing_scam/)

### **The Fog of Cyberwar**

BY: DANNY BRADBURY, THE GUARDIAN  
02/05/2009

Don Jackson, senior security researcher for SecureWorks, believes that recent attacks on Kyrgyzstan came from Russian hackers, and says that the malicious traffic came almost completely from Russian networks that are controlled by the Russian Business Network, who are notorious for conducting cyber attacks. Jackson explains that he thinks the attacks were motivated by Russian pressure to Kyrgyz opposition, which has been critical of closing a U.S. airbase that Russia would like to see closed. Some experts, however, believe that Kyrgyzstan leadership hired Russian hackers to carry out the attacks to silence its own opposition.

<http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access>



### **Are 'Cyber-Militias' Attacking Kyrgyzstan?**

BY: ROBERT MACKEY, THE LEDE  
02/05/2009

Kyrgyzstan was recently the target of a two-week assault from a cyber-militia based in Russia that hit Kyrgyzstan's Internet service with massive distributed denial of service attacks. The attacks forced Kyrgyzstan Web sites to shut down by targeting the two main Internet service providers in the country that account for 80 percent of the country's bandwidth. Experts claim that the attacks were almost identical to those on Georgian Web sites in August of 2008. Although most security experts feel that the attacks came from hackers in Russia, the article explains how some experts feel that Russia may be falsely accused for the attacks.

<http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/>

### **DDoS Attack Boots Kyrgyzstan From Net**

BY: DAN GOODIN, THE REGISTER  
01/28/2009

Attacks from a Russian cybermilitia were able to interrupt online traffic in and out of Kyrgyzstan for more than a week using attacks similar to those used against the republic of Georgia last year. Many of the country's Web services were still unavailable two weeks after the attacks. The hackers used distributed denial of service (DDoS) attacks which flood the victim servers with malicious data until the server is unable to respond to legitimate connection requests. Experts agree that the hackers were most likely Russian citizens who were likely recruited by Russian officials, and the majority of the drones that are launching the attacks are located in Russia.

[http://www.theregister.co.uk/2009/01/28/kyrgyzstan\\_knocked\\_offline/](http://www.theregister.co.uk/2009/01/28/kyrgyzstan_knocked_offline/)

### **Cisco Warns of Four WLAN Controller Vulnerabilities**

BY: JOHN COX, NETWORK WORLD  
02/04/2009

Cisco recently issued a security alert that warned about four vulnerabilities that affect all of its wireless LAN controllers. Three of the vulnerabilities are denial-of-service attacks while the fourth allows attackers to gain administrative rights to the controller. Cisco has also posted software patches for all four of the vulnerabilities. Two of the DoS attacks target Web authentication and the third DoS attack uses certain IP packets to cause the controller to become unresponsive.

<http://www.networkworld.com/news/2009/02/0409-cisco-wlan-vulnerabilities.html>

### **Federal Workers Notified After Virus Breach at Tech Consulting Firm**

BY: ROBERT MCMILLAN, COMPUTER WORLD  
02/03/2009

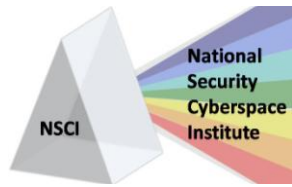
SRA International Inc. has notified their employees of a recent data breach that may have compromised employee information. Hackers planted malicious software that allowed them to gain access to employee information such as names, addresses, social security numbers, dates of birth, and health care provider information. The technology consulting company lists the Department of Defense, Department of Homeland Security and National Guard among its clients. The malware was not detected by the company's antivirus software.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127264>

### **Troubled Ukrainian Host Sidelined**

BY: BRIAN KREBS, WASHINGTON POST  
01/30/2009

UkrTeleGroup Ltd., a Ukrainian Web hosting provider that hosted malicious software, was



recently taken offline following abuse reports from Security Fix to the company's Internet provider. The company hosted hundreds of servers that control networks of computers that were infected with variants of "DNSChanger," a Trojan horse program that intercepts traffic flowing to and from the infected computer. The controllers of DNSChanger could intercept personal and financial information, and block infected computers from visiting security-related Web sites that could help victims remove the malicious software.

[http://voices.washingtonpost.com/securityfix/2009/01/troubled\\_ukrainian\\_host\\_sideli.html](http://voices.washingtonpost.com/securityfix/2009/01/troubled_ukrainian_host_sideli.html)

### **Less Than 10 Percent of E-mail in 2008 Was Non-malicious**

SECURITYPARK.NET  
01/29/2009

Panda Security's TrustLayer Mail service, recently released data that found that of 430 million mail messages that were evaluated, 89.88% were spam and 1.11% was infected with malware. The research claimed that the most common spam subjects in 2008 were sexual performance enhancers and pharmaceuticals, and spam levels peaked in the year's second quarter at 94.27% of all mail reaching organizations. The Netsky.P worm was the most frequently identified malicious code from spam messages in 2008, although the Rukap.G backdoor Trojan and the Dadobra.BI Trojan were also prevalent.

[http://www.securitypark.co.uk/security\\_article\\_262568.html](http://www.securitypark.co.uk/security_article_262568.html)

### **Indian Embassy Web site Hack Part of Wider Assault**

BY: JOHN LEYDEN, THE REGISTER  
01/29/2009

Researchers Ismael Valenzuela and Dancho Danchev report that the Indian Embassy in Spain has been spreading malware because of an injected malicious iFrame. The attack on the

Indian Embassy is part of a wider code injection push that experts believe could be a part of an early massive malware attack. Code inserted into the compromised websites links visitors to illicit pharmaceutical websites, and the attack is similar to previous assaults on the Times of India website and the Pravda website in Russia. [http://www.theregister.co.uk/2009/01/29/indian\\_embassy\\_website\\_hack/](http://www.theregister.co.uk/2009/01/29/indian_embassy_website_hack/)

### **SQL Server Database Hack Tricks Forensics**

BY: KELLY JACKSON HIGGINS, DARK READING  
01/29/2009

Security researcher Cesar Cerrudo will demonstrate how hackers may be able to circumvent forensics investigations by covering his tracks in a sophisticated SQL Server database attack. Cerrudo explains that hackers could load external libraries or binary code to manipulate the server or use buffer overflow attacks, and says that any database could be manipulated with these antforensics techniques. Attackers could even leave behind false evidence that leads to the victim organization's database administrator, and Cerrudo recommends that organizations use a third-party monitoring system, perform regular patching and vulnerability scans, and use strong passwords.

<http://www.darkreading.com/security/attacks/showArticle.jhtml;jsessionid=TE02RZHUE0WNGQSNL0SKHSCJUNN2JVN?articleID=212903514>

### **What the Heartland Data Breach Tells Us**

BY: LUTHER MARTIN, HELP NET SECURITY  
01/29/2009

Experts believe that the recent data breach at Heartland Payment Systems proves that there needs to be stronger security standards for credit card numbers and other sensitive information. Credit card information handlers currently must comply with the Payment Card Industry Security Standard, but many argue that the standards are not strong enough.

Researchers recently released a paper, "An



Inquiry into the Nature and Cause of the Wealth of Internet Miscreants,” that found that credit card numbers are sold by cyber-criminals over other sensitive information by 20 to 1. The attacks on Heartland also show that security does not need to simply keep hackers outside of networks; there must also be better security measures for protecting information inside the network.

<http://www.net-security.org/article.php?id=1202>

### **Heartland Sniffer Hid In Unallocated Portion of Disk**

BY: EVAN SCHUMAN, STOREFRONT BACKTALK  
01/28/2009

Heartland CFO Robert Baldwin explains that the malware that stole payment card information from card processor Heartland Payment Systems was so well hidden in an unallocated portion of a server’s disk, that it eluded two teams of forensic investigators. Experts say that the way that the files were hidden are indicative of a highly sophisticated attack because hiding file sin unallocated disk space requires a high level of access and skill in manipulating operating systems. Heartland announced in January that it will form a department that will work exclusively to develop end-to-end

encryption to prevent future theft of sensitive information.

<http://www.storefrontbacktalk.com/securityfraud/heartland-sniffer-hid-in-unallocated-portion-of-disk/>

### **Indian Hackers Caught in Hong Kong**

BY: NICK FARRELL, IT EXAMINER  
01/29/2009

Two Indian Hackers, Jaisankar Marimuthu and Thirugnanam Ramanathan, were arrested in Hong Kong and charged with coordinating an online scam to break into brokerage companies. A third man, Chockalingam Rmanathan is still on the run. The hackers posed as online traders and bought shares of stocks that they already owned at inflated prices to drive up the price of the stock. The criminals made more than \$120,000, and cost the share broker that they were posing as more than a million dollars. The U.S. government has requested the extradition of the criminals to face charges.

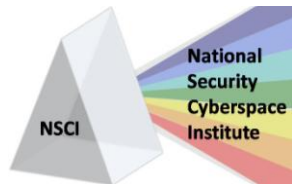
<http://www.itexaminer.com/indian-hackers-caught-in-hong-kong.aspx>



### **Intelligent Software Solutions**

ISS is a leading edge software solution provider for enterprise and system data, services, and application challenges. ISS has built hundreds of operationally deployed systems, in all domains – “From Space to Mud”™.

With solutions based upon modern, proven technology designed to capitalize on dynamic service-oriented constructs, ISS delivers innovative C2, ISR, Intelligence, and cyber solutions that work today and in the future. <http://www.issinc.com>.



## CYBERSPACE TACTICS AND DEFENSE

### Verizon Expands DoS Defenses in 24 Countries

BY: MATT HAMBLÉN, COMPUTERWORLD  
02/10/2009

Verizon Business recently announced that it has added a detection component to its DoS Defense service that will combat DoS attacks. The DoS Defense program is currently in use in 22 countries in Europe and Asia, and Verizon already offers mitigation services in the United States. The mitigation and detection services are managed in the cloud over the Verizon IP network and works by scanning Internet traffic for suspicious activity, while the mitigation component can redirect malicious traffic away from a client's network. AT&T also offers defense services, but Verizon's customers extend into more countries than AT&T and "provides a superior interface for tracking alerts and problems."

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127548>

### Secure Your Communications Against Cyber Warfare

SECURITY PARK  
02/02/2009

As organizations are increasingly sharing information over a vast number of IT systems and databases, the information is becoming more at risk of data breaches or abuse. Risks range from careless users who may lose a disk or USB drive containing sensitive information, to foreign intelligence services that use cyber warfare techniques against other nations. The article explains how an accurate risk assessment is the most important step for organizations to secure their communications.

[http://www.securitypark.co.uk/security\\_article\\_262563.html](http://www.securitypark.co.uk/security_article_262563.html)

### Metasploit Hacking Tool To Add New Services-Based Features

BY: KELLY JACKSON HIGGINS, DARK READING  
02/09/2009

The new Metasploit hacking tool will aim to add back-end services such as an "opcode" database client and a password cracker to expand the tool's resources for users. Adding these services to the current tool will hopefully increase the commercial penetration testing product market by offering enterprises with low-cost options for penetration testing. Other companies, such as Core Security Technologies, are looking into adding penetration testing services. Some experts are concerned that criminal hackers could abuse the Metasploit services to crack passwords and develop attacks.

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml;jsessionid=1KLECJQGRCX2SQSNDLRSKHSCJUNN2JVN?articleID=213401744>

### Coming Soon: Full-disk Encryption For All Computer Drives

BY: LUCAS MEARIAN, COMPUTER WORLD  
01/27/2009

The six largest computer drive manufacturers recently released specifications for full-disk encryption standards that will be used for hard disk drives, solid state drives, and encryption key management applications. The specifications include: the Opal Specification, which outlines requirements for storage devices; the Enterprise Security Subsystem Class Specification, which addresses security in data centers and high-volume applications; and the Storage Interface Interactions Specification, which details how the new standards will interact with existing specifications.

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126869&intsrc=hm\\_ts\\_head](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126869&intsrc=hm_ts_head)



### **Banks, Credit Unions Scramble in Wake of Heartland Breach**

BY: JAIKUMAR VIJAYAN, COMPUTER WORLD  
01/27/2009

Banks and credit unions nationwide have reissued thousands of credit and debit cards following the disclosure of the recent data breach at Heartland Payment Systems. There has also already been a lawsuit filed on behalf of a victim of the breach, who is claiming that Heartland was negligent in protecting cardholder information. Heartland has not released the number of cards that were compromised in the attack, but has said that they discovered the breach after receiving notifications from Visa and MasterCard about suspicious transaction activity.

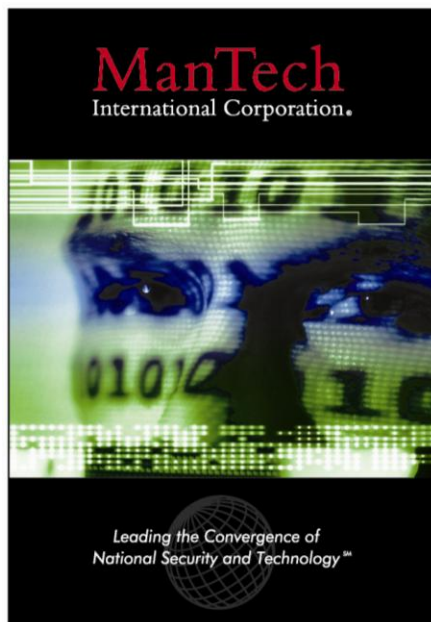
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9126879>

### **Securing Social Networks, from Facebook to Myspace to LinkedIn**

BY: BRIAN PRINCE, EWEK  
02/07/2009

Security researchers Nathan Hamiel and Shawn Moyer spoke at the ShmooCon 2009 conference in Washington, D.C., and presented examples of attacks on social networking sites such as Myspace and Facebook. Hamiel says that social networking sites should improve their default privacy settings and warns that most of the sites' users do not understand security practices. Both researchers emphasized the importance of educating users about possible threats and providing security tips. Hamiel also said that users that link to offsite content from social networking sites could be infected with malicious code.

<http://www.eweek.com/c/a/Security/Securing-Social-Networks-From-Facebook-to-MySpace-to-LinkedIn/?kc=rss>



### ***ManTech's Cyber Solution Center Helps Combat Threats to our National Infrastructure***

**ManTech International Corporation** is a leading provider of innovative technologies and solutions for mission-critical national security programs for the Intelligence Community; the departments of Defense, State, Homeland Security and Justice; the Space Community and other U.S. federal government customers. It has recently established a Cyber Solution Center that marshals expertise from across the company to help the U.S. government and private industry fight the increasing threats to our IT and communications infrastructure. ManTech has been providing cyber operations services to the U.S. government and private industry for 11 years and its cyber security professionals have authored books and articles on honeypots (catching hackers), service oriented architecture security and network security monitoring. They have also taught for leading cyber security education providers such as SANS, Foundstone, USENIX, HTCIA and Black Hat. For additional information on ManTech's Cyber Solutions contact Mark Root at: [mark.root@ManTech.com](mailto:mark.root@ManTech.com)



### CYBERSPACE - LEGAL

#### **FBI Investigates \$9 Million ATM Scam**

BY: JOHN DEUTZMAN, FOX NEWS  
02/02/2009

According to Fox News, criminals behind an international ATM scam may have stolen more than \$9 million and gained access to sensitive information from people around the world. The entire scam took place in just a few hours in 29 cities including New York, Montreal, Moscow, and Hong Kong. FBI Agent Ross Rice reports that they have never seen an ATM fraud scam of this scale. Criminals hacked into the computer system for RBS WorldPay, and were able to steal information that allowed them to duplicate ATM cards. Hackers were also able to somehow bypass the withdraw limits on the cards, and used only 100 cards to steal the \$9 million. The FBI does not have any suspects so far, and an Atlanta attorney has already filed a lawsuit against RBS WorldPay for not protecting personal information.

[http://www.myfoxny.com/dpp/news/090202\\_FBI\\_Investigates\\_9\\_Million\\_ATM\\_Scam](http://www.myfoxny.com/dpp/news/090202_FBI_Investigates_9_Million_ATM_Scam)

#### **IT Worker Indicted for Setting Malware Bomb at Fannie Mae**

BY: TIM WILSON, DARK READING  
01/29/2009

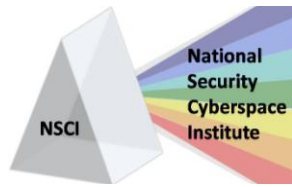
A federal grand jury in Maryland recently indicted Rajendrasinh Babubhai Makwana, who attempted to crash 4,000 servers at Fannie Mae after being terminated. Makwana infected the company's servers with a malicious script that could have wiped out all of the passwords on the servers, replace all of the Fannie Mae data with zeros, and destroy the backup software on the servers. Court documents also report that the malicious script could have removed software from critical servers, and power off all of the company's servers. The complaint says that the malicious script would have caused millions of dollars of damage and shut down operations at Fannie Mae for at least a week. Makwana is facing a maximum sentence of ten years in prison.

<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212903570>

**ITT CORPORATION**  
**Cyber Assurance Department**  
ADVANCED ENGINEERING & SCIENCES

Our goal is to design, develop, evolve and transition information technology solutions and provide engineering services in response to cross-domain information sharing, information assurance and cyber security requirements.

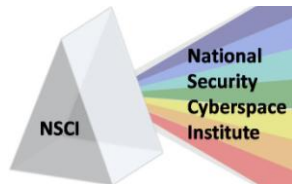
474 Pheonix Dr.  
Rome, NY 13441  
315 838 7000  
aes.itt.com



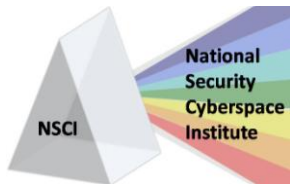
## CYBERSPACE-RELATED CONFERENCES

**Note: Dates and events change often. Please visit web site for details.** Please provide additions, updates, and/or suggestions for the CYBER calendar of events [here](#).

16 – 19 Feb 2009	<b>Black Hat DC 2009</b> , Washington DC, <a href="http://www.blackhat.com/">http://www.blackhat.com/</a>
5 – 6 Mar 2009	<b>Warfighter’s Vision Conference 2009</b> , Washington, DC, <a href="http://www.afei.org/">http://www.afei.org/</a>
9 – 11 Mar 2009	<b>INFOSEC World Conference &amp; Expo</b> , Orlando FL, <a href="http://www.misti.com/default.asp?page=65&amp;Return=70&amp;ProductID=5539">http://www.misti.com/default.asp?page=65&amp;Return=70&amp;ProductID=5539</a>
13 – 15 Mar 2009	<b>Cybercultures: Exploring Critical Issues</b> , Salzburg Austria, <a href="http://www.inter-disciplinary.net/ci/Cyber/cybercultures/c4/fd.html">http://www.inter-disciplinary.net/ci/Cyber/cybercultures/c4/fd.html</a>
17 – 18 Mar 2009	<b>Atlanta SecureWorld Expo</b> ; Atlanta, GA; <a href="http://secureworldexpo.com/events/index.php?id=252">http://secureworldexpo.com/events/index.php?id=252</a>
23 - 27 Mar 2009	<b>FAA IT/ISS 2009</b> , Dallas, Texas, <a href="https://itissconference.faa.gov/">https://itissconference.faa.gov/</a>
25 – 26 Mar 2009	<b>Boston SecureWorld Expo</b> ; Boston, MA; <a href="http://secureworldexpo.com/events/index.php?id=251">http://secureworldexpo.com/events/index.php?id=251</a>
26 – 27 Mar 2009	<b>4<sup>th</sup> International Conference on Information Warfare and Security</b> , Cape Town, South Africa, <a href="http://www.ktn.qinetiq-tim.net/events.php?page=ev_eventfull&amp;item=1">http://www.ktn.qinetiq-tim.net/events.php?page=ev_eventfull&amp;item=1</a>
30 Mar – 2 Apr 2009	<b>Computational Intelligence in Cyber Security</b> , Nashville TN, <a href="http://www.ieee-ssci.org/index.php?q=node/21">http://www.ieee-ssci.org/index.php?q=node/21</a>
6 – 8 Apr 2009	<b>Cyber Security and Information Intelligence Workshop</b> , Oak Ridge National Laboratory, <a href="http://www.ioc.ornl.gov/csiirw07/">http://www.ioc.ornl.gov/csiirw07/</a>
7 – 8 Apr 2009	<b>2009 USSTRATCOM Cyberspace Symposium</b> , Omaha, NE, <a href="http://www.afcea.org/events/stratcom/introduction.asp">http://www.afcea.org/events/stratcom/introduction.asp</a>
13 – 15 Apr 2009	<b>Cyber Security and Information Infrastructure Research Workshop</b> , Oak Ridge National Lab, TN, <a href="http://www.ioc.ornl.gov/csiirw07/">http://www.ioc.ornl.gov/csiirw07/</a>
14 – 17 Apr 2009	<b>Black Hat Europe</b> , Amsterdam The Netherlands, <a href="http://www.blackhat.com/">http://www.blackhat.com/</a>
20 – 24 Apr 2009	<b>RSA Conference</b> , San Francisco CA, <a href="http://www.rsaconference.com/2009/US/Home.aspx">http://www.rsaconference.com/2009/US/Home.aspx</a>
30 Apr – 1 May 2009	<b>Terrorism, Crime &amp; Business Symposium</b> , Houston, TX, <a href="http://www.stmarytx.edu/ctl/content/events/Business_Symposium.html">http://www.stmarytx.edu/ctl/content/events/Business_Symposium.html</a>
4 – 8 May 2009	<b>Army Global Information Operations (IO) Conference</b> , Colorado Springs, CO
6 – 7 May 2009	<b>Philadelphia SecureWorld Expo</b> ; Philadelphia, PA; <a href="http://secureworldexpo.com/events/index.php?id=253">http://secureworldexpo.com/events/index.php?id=253</a>
11 – 15 May 2009	<b>2009 Department of Energy Cyber Security Conference</b> , Henderson, NV, <a href="http://cio.energy.gov/csc_conference.htm">http://cio.energy.gov/csc_conference.htm</a>
13 – 14 May 2009	<b>Cyber Defence</b> , Stockholm, Sweden, <a href="http://www.smi-online.co.uk/events/overview.asp?is=1&amp;ref=3080">http://www.smi-online.co.uk/events/overview.asp?is=1&amp;ref=3080</a>
21 May 2009	<b>Systemic Approaches to Digital Forensic Engineering (SADFE)</b> , Oakland, CA, <a href="http://conf.ncku.edu.tw/sadfe/">http://conf.ncku.edu.tw/sadfe/</a>
24 – 28 May 2009	<b>Internet Monitoring and Protection</b> , Venice Italy, <a href="http://www.iaria.org/conferences2009/SECURWARE09.html">http://www.iaria.org/conferences2009/SECURWARE09.html</a>
26 – 29 May 2009	<b>Network Centric Warfare Europe</b> , Cologne, Germany, <a href="http://www.asdevents.com/event.asp?ID=358">http://www.asdevents.com/event.asp?ID=358</a>
2 – 5 Jun 2009	<b>Applied Cryptography and Network Security (ACNS)</b> , Paris-Rocquencourt, France, <a href="http://acns09.di.ens.fr/">http://acns09.di.ens.fr/</a>
7 – 10 Jun 2009	<b>Information Hiding Workshop</b> , Darmstadt, Germany, <a href="http://www.ih09.tu-darmstadt.de/">http://www.ih09.tu-darmstadt.de/</a>



14 – 18 Jun 2009	<b>IEEE International Conference on Communications (ICC) 2009</b> , Dresden, Germany, <a href="http://www.comsoc.org/confs/icc/2009/index.html">http://www.comsoc.org/confs/icc/2009/index.html</a>
14 – 19 Jun 2009	<b>International Conference on Emerging Security Information, Systems and Technologies</b> ; Athens Greece, <a href="http://www.iaria.org/conferences2009/SECURWARE09.html">http://www.iaria.org/conferences2009/SECURWARE09.html</a>
16 - 18 Jun 2009	<b>Air Force Cyberspace Symposium 2009</b> , Bossier City, Shreveport, LA, <a href="http://www.cyberspacesymposium.com/">http://www.cyberspacesymposium.com/</a>
22 – 24 Jun 2009	<b>Information Operations Europe 2009: Delivering Effects Through Influence Activity</b> , London, UK, <a href="http://www.defenceiq.com/ShowEvent.aspx?id=173906">http://www.defenceiq.com/ShowEvent.aspx?id=173906</a>
25 – 26 Jun 2009	<b>Workshop on Digital Forensics &amp; Incident Analysis</b> , Athens, Greece, <a href="http://www.wdfia.org/">http://www.wdfia.org/</a>
28 Jun – 3 July 2009	<b>Annual Computer Security Incident Handling Conference (FIRST)</b> , Kyoto, Japan, <a href="http://www.first.org/conference/">http://www.first.org/conference/</a>
1 – 3 Jul 2009	<b>Australasian Conference on Information Security and Privacy (ACISP)</b> , Brisbane, Australia, <a href="http://conf.isi.qut.edu.au/acisp2009/">http://conf.isi.qut.edu.au/acisp2009/</a>
6 – 7 Jul 2009	<b>European Conference on Information Warfare and Security (ECIW)</b> , Lisbon, Portugal, <a href="http://www.academic-conferences.org/eciw/eciw2009/eciw09-home.htm">http://www.academic-conferences.org/eciw/eciw2009/eciw09-home.htm</a>
6 – 8 Jul 2009	<b>4<sup>th</sup> Global Conference: Visions of Humanity in Cyberculture, Cyberspace and Science Fiction</b> , Oxford, United Kingdom, <a href="http://www.inter-disciplinary.net/ati/Visions/v4/cfp.html">http://www.inter-disciplinary.net/ati/Visions/v4/cfp.html</a>
7 – 10 Jul 2009	<b>Conference on Ubiquitous Intelligence and Computing</b> , Brisbane, Australia, <a href="http://www.itee.uq.edu.au/~uic09/">http://www.itee.uq.edu.au/~uic09/</a>
25 – 30 July	<b>Black Hat USA 2009</b> , Las Vegas NV, <a href="http://www.blackhat.com/">http://www.blackhat.com/</a>
July 2009	<b>International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)</b> , Milan, Italy, <a href="http://www.dimva.org/">http://www.dimva.org/</a>
17 – 19 Aug 2009	<b>Digital Forensics Research Workshop</b> , Montreal, Canada, <a href="http://www.dfrws.org/">http://www.dfrws.org/</a>
18 – 20 Aug 2009	<b>International Conference on Information Assurance and Security</b> , Xi'an, China, <a href="http://www.ias09.org/">http://www.ias09.org/</a>
31 Aug – 4 Sep 2009	<b>6<sup>th</sup> International Conference on Trust, Privacy &amp; Security in Digital Business</b> , Linz, Austria, <a href="http://www.icsd.aegean.gr/trustbus2009/">http://www.icsd.aegean.gr/trustbus2009/</a>
29 – 30 Sep 2009	<b>Detroit SecureWorld Expo</b> ; Detroit, MI; <a href="http://secureworldexpo.com/events/index.php?id=257">http://secureworldexpo.com/events/index.php?id=257</a>
28 – 29 Oct 2009	<b>Seattle SecureWorld Expo</b> ; Seattle, WA; <a href="http://secureworldexpo.com/events/index.php?id=249">http://secureworldexpo.com/events/index.php?id=249</a>
4 – 5 Nov 2009	<b>Dallas SecureWorld Expo</b> ; Dallas, TX; <a href="http://secureworldexpo.com/events/index.php?id=250">http://secureworldexpo.com/events/index.php?id=250</a>
18 – 20 Nov 2009	<b>MINES 2009 International Conference on Multimedia Information Networking and Security</b> , Wuhan, China; <a href="http://liss.whu.edu.cn/mines2009/">http://liss.whu.edu.cn/mines2009/</a>



## EMPLOYMENT OPPORTUNITIES WITH NSCI

<u>Job Title</u>	<u>Location</u>
<a href="#">Operational Deterrence Analyst</a>	NE, VA
<a href="#">Defensive Cyber Ops Analyst</a>	NE, VA, CO
<a href="#">Cyber SME</a>	NE, VA, TX, CO
<a href="#">Geospatial Analyst</a>	NE
<a href="#">Logistics All-Source Intelligence Analyst</a>	NE
<a href="#">SIGINT Analyst</a>	NE, CO
<a href="#">Cyber Operations SME</a>	NE
<a href="#">Website Maintainer</a>	NE
<a href="#">Cyberspace Specialists</a>	NE
<a href="#">Cyberspace Manning IPT</a>	NE

## CYBERPRO CONTENT / DISTRIBUTION

<p><b>Officers</b></p> <p>President <a href="#">Larry K. McKee, Jr.</a></p> <p>Senior Analyst <a href="#">Jim Ed Crouch</a></p> <p>-----</p> <p>CyberPro Editor-in-Chief <a href="#">Lindsay Trimble</a></p> <p>CyberPro Research Analyst <a href="#">Kathryn Stephens</a></p> <p><a href="#">CyberPro Archive</a></p>	<p>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.</p> <p>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 <a href="#">National Security Cyberspace Institute</a>.</p>
<p>To subscribe or unsubscribe to this newsletter click here <a href="#">CyberPro News Subscription</a>.</p> <p>Please contact <a href="#">Lindsay Trimble</a> regarding CyberPro subscription, sponsorship, and/or advertisement.</p>	

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