

# CyberPro

Volume 1, Edition 12  
October 23, 2008

## Keeping Cyberspace Professionals Informed

<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 Research Analyst <a href="#">Kathryn Stephens</a></p> <p><a href="#">CyberPro Archive</a></p>	<p><i>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.</i></p> <p><i>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>.</i></p>
<p>To subscribe or unsubscribe to this newsletter click here <a href="#">CyberPro News Subscription</a>.</p> <p>Please contact <a href="#">Larry McKee</a> , ph. (757) 871-3578, 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 CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.**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

<b>Table of Contents .....</b>	<b>2</b>
<b>Cyberspace Big Picture .....</b>	<b>5</b>
Next president will need to make cybersecurity a priority, experts say .....	5
The Cyber Attack Danger .....	5
'Open Wide...' .....	5
Lords to attack UK.gov failings on internet security.....	6
Cyber security threats grow in sophistication, subtlety and power .....	6
FBI: Several nations eye U.S. cybertargets.....	6
Super Cyber Command.....	7
SKorean PM warns of hacking threat by NKorea, China .....	7
The Internet's Top 10 Most Controversial Figures of 2008 .....	7
WhiteHat Enhances Education Services .....	7
IT security guide: Understanding cyber-risks means knowing what questions to ask .....	8
Users and vendors should team up over cybersecurity .....	8
Security Assurance Sometimes Starts From the Outside In .....	8
US proposes ways to make DNS servers more secure .....	8
Big changes ahead for the Internet, says Vint Cerf .....	9
The Trouble With 'Deep Packet Inspection' .....	9
It's All About the PII Now .....	9
ANSI Launches Guide to Help Calculate Cyber Security Risk.....	9
LM Establishes Center for Cyber Security Innovation .....	10
Another View   Getting the facts straight on cybersecurity .....	10
<b>Cyberspace: Department of Homeland Security (DHS) .....</b>	<b>10</b>
Senators propose changes at DHS .....	10
DHS secretary pushes industry to invest in cybersecurity .....	11
Chertoff: No Big Brother approach to 'Net security for DHS .....	11
Chertoff Urges More Cooperation to Protect Nation's Critical Computer Systems .....	11
Cybersecurity No Longer a "Stepchild," says DHS Chief .....	12
DHS not prepared for cyberattacks, House committee chair says.....	12
Report: Homeland Security network has problems .....	12
<b>Cyberspace: Department of Defense (DoD) .....</b>	<b>12</b>
Military Needs Hackers, Stratcom Chief Says .....	12
The right stuff for cyber warfare.....	13



NSA shows the way to develop secure systems .....	13
U.S. Army gets tough with desktop software policy.....	13
New command coming to Ft. Gordon .....	13
HSPD-12 card may promote information sharing.....	14
USAF Cyber Command Whittling Down List of Possible Bases .....	14
Shelton: Integrate Space and Cyber Ops .....	14
Air Force demotes Cyberspace Command .....	14
OP-ED: Cyber is bigger than Barksdale .....	15
Cyber change is 'streamlining' .....	15
<b>Cyberspace Lessons Learned .....</b>	<b>15</b>
Lessons Learned From Cyber Storm II .....	15
Security Lessons from the World Bank Breach .....	16
<b>Cyberspace Research: Findings and Opportunities .....</b>	<b>16</b>
Buzz of the Week: Hopes for cybersecurity.....	16
DHS to hold industry day on cyber initiative .....	16
Government Awards Contract for Cyber-Behavior Research .....	16
Air Force lab issues long-term BAA for cyber defense research.....	17
Cellphone Botnets, Blackmailing VOIP & a Healthy Cybercrime Economy .....	17
DISA seeks state-of-the-art security assessment services .....	17
Users, Enterprises Pay for Poor Privacy Policies, Study Says .....	18
Security Software Suites No Match for Custom Attacks .....	18
Botnet experts meet as threat grows for corporations.....	18
Report: Energy Companies Are Top Target of Web-Borne Malware .....	19
Up next: Cellular botnets, cybermilitias .....	19
Georgian cyberattacks suggest Russian involvement, say researchers .....	19
Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.....	19
Spies Launch 'Cyber-Behavior' Investigation .....	20
Study: 80% of Organizations Suffer Breaches, Most From the Inside .....	20
<b>Cyberspace Hacks, Tactics and Defense.....</b>	<b>20</b>
Report: U.S. not prepared for EMP attacks .....	20
Cyber-attack theory as al-Qaida websites close .....	20
IG says Defense systems lack reliable safeguards against hackers.....	21
FTC warns consumers of increase in Internet scams .....	22
Organized cybercrime replaces random individual attacks .....	22
Managing Mercenaries .....	22
NEFA Foundation: Al-Fajr Center Announces Shuttering of Three Top Jihad Web Forums.....	22

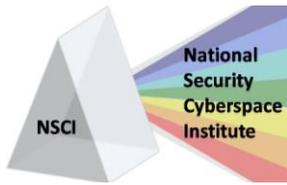


# CyberPro

Volume 1, Edition 12  
October 23, 2008

## Keeping Cyberspace Professionals Informed

New USAF weapon could shut down or damage enemy electronics .....	22
Microsoft under threat from new attack code .....	23
Warezov botnet rises from the grave .....	23
NY tops computer virus threat list.....	23
Third-Party Hack.....	23
Free Tool Hacks Banking, Webmail, and Social Networking Sessions.....	24
Storm May Finally Be Over .....	24
Hackers force Al-Arabiya site name change .....	24
Saudi-owned TV website hit by cyber attack (AFP) .....	24
10,000 LinkedIn users targeted in spear phishing attack .....	25
Metasploit 3.2 Offers More 'Evil Deeds' .....	25
Skype Acknowledges Chinese Spying .....	25
<b>Cyberspace – Legal .....</b>	<b>26</b>
FBI says Dark Market sting netted 56 arrests .....	26
Student gets jail for crashing university servers .....	26
Opinion: FTC's New Red Flag Rules cast wide identity theft net .....	26
German court says IP addresses in server logs are not personal data.....	26
Intellectual Property Bill Becomes Law: Critics Say It Goes Too Far .....	27
<b>Cyberspace-Related Conferences .....</b>	<b>27</b>
<b>CyberPro Content/Distribution .....</b>	<b>28</b>



## CYBERSPACE BIG PICTURE

### Next president will need to make cybersecurity a priority, experts say

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD  
10/22/2008

Officials at the DHS state the increasing danger of cyberattacks will make cybersecurity a top focus for the next presidential administration especially in areas of sector collaboration, security research and development investments, greater White House involvement and the implementation of President Bush's cybersecurity initiative. Andy Purdy, co-director of the International Cyber Center at George Mason University, explains that government and private sector collaboration must be a top priority in the hopes of developing better cyber defense capabilities. Bush's presidential directive recommended improvements to the security of federal systems including multiple federal agencies, including the National Security Agency. Since the issue of the initiative, government Internet access points have been reduced and the network monitoring Einstein program has been improved. Both presidential candidates have expressed cybersecurity a priority. Obama has discussed strengthening federal involvement in cyber issues and appointing a national cyberadvisor who would report to the president; McCain has expressed support for US-CERT and the National Cyber Response Coordination Group.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117803>

### The Cyber Attack Danger

BY: KEVIN COLEMAN, DEFENSE TECH  
10/21/2008

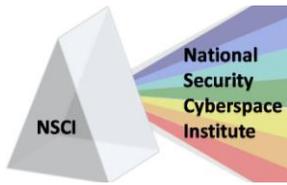
The report lists types of hacker attacks that are expected to cause significant damage according to a cyber threat report released by Intelomics. The list includes social engineering attacks, wireless sniffers, automated widespread denial-of-service attacks, widespread attacks on the DNS, attacks from botnets and zombies, and many more. According to the Congressional Research Service study, cyber attacks now cause more than \$226 billion in damages annually. Because of the increase of attacks and attack methods, as well as the increasing financial consequences of poor security, author Kevin Coleman lists four things that he feels must be done to improve international cybersecurity. These include establishing a threat committee under the U.N. Security Council; determining what constitutes an act of war and forming a legal framework for international cyber crimes; creating a plan of action that can be used against aggressors; and creating a cyber peacekeeping force. The article discusses these and other recommendations in detail.

<http://www.defensetech.org/archives/004478.html>

### 'Open Wide...'

BY: BARRETT SHERIDAN, NEWSWEEK  
10/16/2008

Both Barack Obama and John McCain support digitizing patient files and hospital records to build a comprehensive online patient database, which some say would help doctors have better access to critical patient information and help to save costs. Critics of the plan argue that with open electronic health records, patients could suffer. Insurance companies would have full access to past records and may refuse to cover



## Keeping Cyberspace Professionals Informed

a patient; employers may choose not to hire an applicant based on their health; and there are obvious social consequences for those who have diseases such as AIDS. James Heywood, cofounder of the social networking site PatientsLikeMe.com, claims that open sharing of health information is valuable to both patients and health care professionals. His site allows patients to post their medical information, as well as receive information from others who may have their same disease or experience with medications.

<http://www.newsweek.com/id/164231>

### **Lords to attack UK.gov failings on internet security**

BY: CHRIS WILLIAMS, THE REGISTER  
10/07/2008

The House of Lords Science and Technology Committee discussed the U.K. government's

response to the Committees recommendations for improving personal internet security. Experts and Lords feel that many of the recommendations, such as making software developers legally responsible for vulnerabilities, have gone unrecognized. Lord Broers, chair of the Committee's security sessions, explained that the Government has acted on some recommendations, such as establishing an e-crime police unit which will replace the National Hi-Tech Crime Squad. Lord Broers states the committee will "reassert their calls for better protection" and will continue to monitor Government progress.

[http://www.theregister.co.uk/2008/10/07/lords\\_security\\_debate/](http://www.theregister.co.uk/2008/10/07/lords_security_debate/)



**Georgia Tech Research Institute**  
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.

### **Cyber security threats grow in sophistication, subtlety and power**

BY: JOHN COX, NETWORK WORLD  
10/15/2008

The "Emerging Cyber Threats Report for 2009: Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond" from the Georgia Tech Information Security Center identified the following areas of evolving cybersecurity threats: malware, botnets, cyber warfare, threats to mobile devices and the evolution of the cyber crime economy. The report states that attacks are increasingly

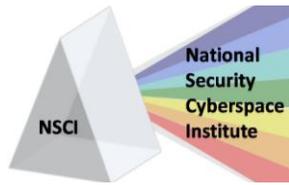
sophisticated in all five areas, and that both industry and government need to become more concerned and security must become more sophisticated to combat threats.

<http://www.networkworld.com/news/2008/10/1508-cybersecurity.html>

### **FBI: Several nations eye U.S. cyber targets**

BY: GRANT GROSS, COMPUTER WORLD  
10/15/2008

Shawn Henry, the assistant director of the FBI's Cyber Investigations division, states there are countries who have developed cyberattack



capabilities and pose a “significant threat” to U.S. cybersecurity. Henry also said that there are currently thousands of open investigations into cybercrime and cyberattacks due to the increasing sophistication of attacks. Henry did not give specific numbers or single out any particular sector, but claims that there is an increase in the use of botnets and organized crime on the Internet. The FBI is currently working to improve information sharing between the government and private sector, and is also working to improve education in areas of cybersecurity.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117258>

### **Super Cyber Command**

BY: BOB BREWIN, GOVERNMENT EXECUTIVE  
10/20/2008

Author, Bob Brewin, states that according to his sources close to the Defense Information Systems Agency, the cyber command will incorporate the DISA network operations center and Homeland Security Department’s National Cyber Security Center. The U.S. Strategic Command will oversee the incorporation of the centers. Cyber missions will go to the three military departments including Air Force Cyber Command, the Navy Cyber Forces Command and provisional Army Network Warfare Battalion.

[http://www.govexec.com/story\\_page.cfm?filepath=/dailyfed/1008/102008wb.htm](http://www.govexec.com/story_page.cfm?filepath=/dailyfed/1008/102008wb.htm)

### **SKorean PM warns of hacking threat by NKorea, China**

THE AGE  
10/15/2008

The South Korean National Intelligence Service warned Prime Minister Han Seung-Soo that over 130,000 bits of government information had been hacked within the last four years. Han met with his cabinet, stating the threat is very

serious and that attacks have originated in both China and North Korea. Han also explained that the information that was stolen was restricted, although not highly confidential, and that the documents focused on foreign policy and national security.

<http://news.theage.com.au/technology/skorean-pm-warns-of-hacking-threat-by-nkorea-china-20081015-50sb.html>

### **The Internet’s Top 10 Most Controversial Figures of 2008**

BY: BRIAN KREBS, POPULAR MECHANICS  
10/08/2008

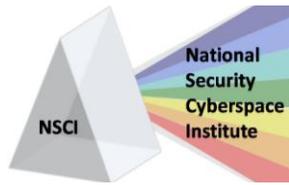
Author, Brian Krebs, writes about ten people who have been important or caused controversy on the Internet this year. For each person, Krebs writes about the subject’s associations, reputation and details about how they caused controversy or why they have been important on the Internet. Not all of the people included are criminals. Some have found security flaws, some have started controversial websites such as wikileaks.org, and some are security researchers.

<http://www.popularmechanics.com/technology/industry/4286458.html>

### **WhiteHat Enhances Education Services**

DARK READING  
10/14/2008

WhiteHat Security is now offering a .Net Security course as part of its Education Services division. WhiteHat is also expanding its current introductory Web Application Security class. The .Net class, which will review coding guidelines for .Net and .Net specific features, is significant because it is the second largest website development platform and has been increasingly targeted for attacks. The expanding Web Applications course will include actual vulnerabilities as examples and will include additional topics such as Cross Site Request Forgery, Business Logic Flaws, and Blind SQL



Injection. The WhiteHat courses aim to “bridge the gap between the security professionals and developers” through education and training.  
[http://www.darkreading.com/document.asp?doc\\_id=165908](http://www.darkreading.com/document.asp?doc_id=165908)

### **IT security guide: Understanding cyber-risks means knowing what questions to ask**

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD  
10/20/2008

The American National Standards Institute (ANSI) released a 40-page guide to help chief financial officers and other executives to prepare for the consequences of cyberattacks. The guide also contained a list of 50 questions to ask an organization’s internal groups as part of a security assessment. The guide recommends asking questions regarding information on required regulations, internal data collection, information destruction practices and penalties for non-compliance. The analysis is expected to help CFOs define cyber risks with monetary terms.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117546>

### **Users and vendors should team up over cybersecurity**

BY: GRANT GROSS, IDG NEWS SERVICE  
10/17/2008

Steve DelBianco, the executive director of NetChoice, explains how Internet users need to be aware of emerging social-engineering attacks, such as the new phishing e-mail scam which claims to be from a financial institution, but actually is harvesting victims’ personal information. DelBianco states there is no “silver bullet” for all levels of security as there are security gaps at each level of the Internet including software, internal network services and operating systems. A report released by NetChoice states tech vendors need to implement more rigid security programs in

coordination with user education. It also states that government agencies need to test the latest technologies and ensure that businesses are implementing security features.

<http://www.techworld.com/news/index.cfm?RSS&NewsID=105849>

### **Security Assurance Sometimes Starts From the Outside In**

SIGNAL MAGAZINE  
10/15/2008

The article discusses the three categories of threats to most organizations which are tools on the desktop, the integration of merged Web content, and configuration flaws. Blake Frantz, chief technology officer for the Center for Internet Security, explains that companies should start from the outside when addressing security issues. This means first looking at areas of the company Web site that does not require identification verification. Then, the company must examine areas where information could be diverted by hackers to fake sites. Finally, the organization must look at what their customers are able to access once they are verified.

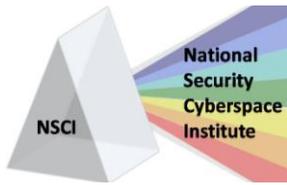
[http://www.afcea.org/signal/articles/templates/signal\\_connections.asp?articleid=1739&zoneid=220](http://www.afcea.org/signal/articles/templates/signal_connections.asp?articleid=1739&zoneid=220)

### **US proposes ways to make DNS servers more secure**

JEREMY KIRK, IDG NEWS SERVICE  
10 OCTOBER 2008

The U.S. government is suggesting records in the DNS root zone be cryptographically signed using Domain Name and Addressing System Security Extensions (DNSSEC), protocols which allow DNS records to carry digital signatures. The U.S. Department of Commerce has requested information on how the DNSSEC would be deployed. Security experts have suggested the use of DNSSEC before, but implementation has been difficult.

Implementation would require domain name



registrars and registries, ISPs and others to upgrade software and configure their systems for digital signature verification. There is also debate over who will manage the cryptographic keys that are required to sign the root file zone. <http://www.techworld.com/news/index.cfm?RSS&NewsID=105605>

### **Big changes ahead for the Internet, says Vint Cerf**

BY: MIKAEL RICKNAS, *IDG NEWS SERVICE*  
10/21/2008

Vint Cerf, vice president at Google, states the internet will increase support for IPv6 which is a more "secure domain name system and international characters". The transition to IPv6 will increase the Internet's address space, allow room for future growth, and require compliance with encryption rules. Cerf explains that there are still implementation problems that must be addressed including the need for more mature network management tools. Cerf states there will be many opportunities for industry with both the IPv6 and the new domain name system security which will use Domain Name System Security Extensions (DNSSEC). <http://www.networkworld.com/news/2008/10/2108-big-changes-ahead-for-the.html?hpg1=bn>

### **The Trouble With 'Deep Packet Inspection'**

BY BOB SULLIVAN, *MSNBC*  
10/16/2008

A new technology, deep packet inspection, makes it easier for an Internet user's surfing behavior to be monitored and tracked. According to a survey published this year by Pointproof, 20% of U.S. companies currently have employees specifically for monitoring employee e-mail and 41% perform some e-mail monitoring. A study by security firm Cyber-Ark reports that more than a third of IT workers admit to using their administrative privileges to access coworkers email and salary information. U.S. ISPs have begun to investigate behavioral

marketing technology, which utilizes deep packet inspection to monitor Internet user behavior. These new technologies have sparked much concern from privacy advocates ultimately resulting in a Congressional hearing which required the ISPs to stop the experiments. <http://redtape.msnbc.com/2008/10/deep-down-most.html>

### **It's All About the PII Now**

BY: JOHN H. SAWYER, *DARK READING*  
10/20/2008

Author, John H. Sawyer, claims that the increase in business security breaches is due to recent security-breach disclosure laws, not the increase of financially motivated cybercrimes and organized crime gangs as many believe. Sawyer explains that recent legal cases are more focused on unauthorized access to personally identifiable information and less about the hacker's motivation or customer notification. Sawyer also writes that companies are more concerned about the financial consequences of data breaches, and worry about a criminal's access to personal information because of the high costs of notifying victims and bad publicity. [http://www.darkreading.com/blog.asp?blog\\_sectionid=447&doc\\_id=166304&WT.svl=blogger1\\_1](http://www.darkreading.com/blog.asp?blog_sectionid=447&doc_id=166304&WT.svl=blogger1_1)

### **ANSI Launches Guide to Help Calculate Cyber Security Risk**

BY: TIM WILSON, *DARK READING*  
10/20/2008

The American National Standards Institute (ANSI) and the Internet Security Alliance have published "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask", which assists companies with determining the risks and costs of data security breaches as well as offering recommendations for preparing for breaches. The guide is the first that has been



issued from a standards group such as ANSI, and is expected to receive much attention by many companies. The guide provides questions which address many topics including: legal compliance; operations; communications; and crisis and risk management. Companies are urged to use their findings on the financial risks of data breaches to determine a course of action to minimize the risks and consequences of breaches.

[http://www.darkreading.com/document.asp?doc\\_id=166276&WT.svl=news1\\_2](http://www.darkreading.com/document.asp?doc_id=166276&WT.svl=news1_2)

### **LM Establishes Center for Cyber Security Innovation**

BY: AEROSPACE & DEFENCE NETWORK  
10/17/2008

Lockheed Martin has announced its new Center for Cyber Security Innovation (CCSI), which aims to expand the company's cyber security capabilities. Rick Johnson, Chief Technology Officer, explains that the Center will not change cyber security practices, but will allow for uniform execution of cyber security solutions across the entire company. Charles Croom will join Lockheed Martin as Vice President of Cyber Security Solutions, and former Senior Executive Service official Lee Holcomb will be the Vice President to lead the CCSI and will also manage technology development initiatives.

[http://www.asd-network.com/press\\_detail\\_B.asp?ID=18115&NID=71163](http://www.asd-network.com/press_detail_B.asp?ID=18115&NID=71163)

### **Another View | Getting the facts straight on cybersecurity**

BY: ROBERT JAMISON, GOVERNMENT COMPUTER NEWS  
10/09/2008

Author, Robert Jamison, writes that the Government Computer News' editorial "Elevate cybersecurity", which discussed conclusions from a study by the Center for Strategic and International Studies' Commission on Cyber Security for the 44th Presidency, were incorrect and misrepresented the facts. Jamison discusses why each of the potential conclusions is not true, and presents the facts which support the progress that the federal government has made in the past year. The conclusions discussed include: the nation's lack of a comprehensive strategy; the CNCI has been overly classified and provides little direction; interaction between the federal government and private sector is inadequate; DHS lacks the capability to oversee cybersecurity efforts; and defense against national threats requires offensive capabilities.

[http://www.gcn.com/online/vol1\\_no1/47332-1.html](http://www.gcn.com/online/vol1_no1/47332-1.html)

## **CYBERSPACE: DEPARTMENT OF HOMELAND SECURITY (DHS)**

### **Senators propose changes at DHS**

BY: REBECCA NEAL, FEDERAL TIMES  
10/08/2008

Senators Joseph Lieberman and Susan Collins state they do not expect full consideration for a bill they are sponsoring regarding changes within the Homeland Security Department to cybersecurity and acquisition, but that they hope to provide a model for the next administration. Lieberman said that the proposed improvements aim to improve the

efficiency and effectiveness of the DHS homeland security efforts. Some of the proposals include: establishment of a consolidated DHS headquarters; improvements to cybersecurity including the establishment of the National Cyber Security Center; appointment of an undersecretary for policy coordination; and appoint a director for operational testing.

<http://www.federaltimes.com/index.php?S=3762341>



### **DHS secretary pushes industry to invest in cybersecurity**

BY: JILL R. AITORO, GOVERNMENT EXECUTIVE  
10/15/2008

During a forum at the U.S. Chamber of Commerce, Homeland Security Secretary Michael Chertoff said that cybersecurity must be shared responsibility between government and industry. Chertoff explains the three areas that the government is focusing on which include: threat detection and mitigation,

education in an effort to reduce threats, and improving security in global supply chains. DHS plans to work with industry to improve cybersecurity, most notably with the release of the National Infrastructure Protection Plan which outlines roles and responsibilities for both government and private industry in critical infrastructure protection.

<http://www.govexec.com/dailyfed/1008/101508j1.htm>



### **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>.

### **Chertoff: No Big Brother approach to 'Net security for DHS**

BY: JULIAN SANCHEZ, ARS TECHNICAL  
10/14/2008

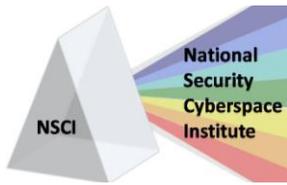
Homeland Security Secretary Michael Chertoff discussed the implementation of the Comprehensive National Cybersecurity Initiative at a briefing with a small group of bloggers and journalists. Chertoff discussed a modest agenda which helped reassure some that the DHS would not be taking a Big Brother approach to securing the government. Chertoff explained the Department has been allotted over \$300 billion for cybersecurity which will go to the government's intrusion detection software, Einstein II, as well as hiring trained programmers and personnel for cybersecurity operations. Chertoff also discussed the recent reduction of government access points to the Internet and the government's efforts to develop a program which could automatically detect and stop potential attacks.

<http://arstechnica.com/news.ars/post/20081014-chertoff-no-big-brother-approach-to-net-security-for-dhs.html>

### **Chertoff Urges More Cooperation to Protect Nation's Critical Computer Systems**

BY: DAVE HENDRICKS, INFOZINE  
10/15/2008

Chertoff states the government must cooperate more with the private sector, who owns the majority of the Internet's infrastructure. Chertoff also said the three major security threats are insider threats, hacking, and supply chain sabotage. Chertoff explains that the government could suggest that private companies use government technology to secure their networks, but is unable to require use of certain software or information sharing. Chertoff also states the government has taken steps to correct its own security flaws, including reducing access points and the coming implementation of the intrusion detection system, Einstein 2. Finally, Chertoff said that the



next step in securing government networks must be a system that will automatically detect and possibly stop attacks.

<http://www.infozine.com/news/stories/op/storiesView/sid/31329/>

### **Cybersecurity No Longer a “Stepchild,” says DHS Chief**

BY MICHAEL GIPS, SECURITY MANAGEMENT  
10/16/2008

In a cybersecurity forum this month, U.S. Department of Homeland Security Michael Chertoff explains that cybersecurity is no longer a “stepchild” of IT, and states that he sees an increasing interest in electronic system protection among young people. Chertoff also makes recommendations for the government, including closing connection points and requiring US-CERT to improve security over all the government’s civilian domains. Chertoff also speaks about the importance of collaboration with the private-sector in areas of technology development, education, recruitment and standards development.

<http://www.securitymanagement.com/news/cybersecurity-no-longer-stepchild-says-dhs-chief-004752>

### **DHS not prepared for cyberattacks, House committee chair says**

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK  
10/13/2008

Rep. Bennie Thompson (D-Miss.), chairman of the House Homeland Security Committee, states the Department is behind schedule

regarding preparation for cyber and explosive attacks. In a letter to DHS Secretary Michael Chertoff, Thompson said the department has only completed the first step of planning on one of eight planning scenarios which were included in the National Response Framework. None of the eight scenarios have complete strategic plans, operation concepts or operational plans. Thompson also asked for the department to complete a schedule by Oct. 23 for the completion of the planning scenarios and guidance documents.

<http://www.fcw.com/online/news/154055-1.html>

### **Report: Homeland Security network has problems**

BY: EILEEN SULLIVAN, THE ASSOCIATED PRESS  
10/08/2008

The Homeland Security Department is working to replace the \$91 million Homeland Security Information Network, which was launched in 2004 to provide a system for securely sharing terrorism information among the government and private industry. The original system had multiple flaws and was difficult to navigate. The Government Accountability Office has said that plans for the new network are “not clear” which may cause “delays and higher costs”. The Departments plans to move users to the new network starting in May 2009.

[http://www.siliconvalley.com/latestheadlines/ci\\_10670772](http://www.siliconvalley.com/latestheadlines/ci_10670772)

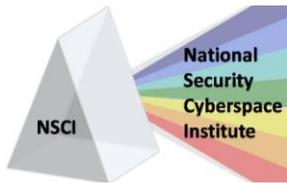
## **CYBERSPACE: DEPARTMENT OF DEFENSE (DOD)**

### **Military Needs Hackers, Stratcom Chief Says**

BY: WILLIAM MCMICHAEL, ARMY TIMES  
10/02/2008

The military is looking for cyber-qualified personnel who can defend .mil and .smil

domains, but also launch cyber attacks against enemies if necessary. Air Force Gen. Kevin Chilton, chief the U.S. Strategic Command, explained that the military must develop offensive capabilities in all domains, including offensive cyber operations. Recommendations



for cross-domain attacks were included in the National Military Strategy for Cyberspace Operations. The article also discusses the recent “muscle-flexing” of Russia, stating that Russia

### **The right stuff for cyber warfare**

BY: SEAN GALLAGHER, DEFENSE SYSTEMS  
MAGAZINE  
10/20/2008

Defense Systems Editor-in-Chief Sean Gallagher spoke with Gen. Kevin Chilton, Air Force Commander of the Strategic Command regarding U.S. cyber operations priorities. Defense Systems asked Chilton about consolidation of cyber operations, improvements in cyber operations integration, and key technologies which will aid in building cyber capabilities. Chilton compares the current cyber issues with the issues facing the space domain 15 years ago, and states that the military is prioritizing finding new technologies to improve cyber capabilities.

<http://defensesystems.com/Articles/2008/09/Biometrics-Task-Force-reveals-2009-research-funding-areas.aspx>

### **NSA shows the way to develop secure systems**

NET SECURITY  
10/06/2008

The U.S. National Security Agency commissioned a research project by Tokeneer to improve security assurance by using SPARK Ada language and AdaCore’s GNAT Pro environment. The project, which was released to the open source community, demonstrates how security software development can be more cost efficient including improvements to current industrial practices. The goal of the project, which is aimed at both industry and academia, was to improve NSA contractor’s development practices as well as provide a platform for program verification research and education. The article also provides the link to

seems to be acting more offensively, reminiscent of the aggressive Soviet past.  
[http://www.armytimes.com/news/2008/09/military\\_chilton\\_093008w/](http://www.armytimes.com/news/2008/09/military_chilton_093008w/)

project materials including designs, source code, and proofs.

<http://www.net-security.org/secworld.php?id=6619>

### **U.S. Army gets tough with desktop software policy**

BY: ELLEN MESSMER, NETWORK WORLD  
10/07/2008

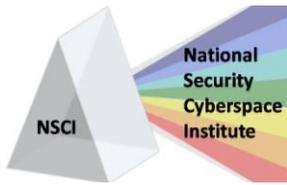
The U.S. Army Information Management Support Center has worked this year to deploy software to 11,000 Army machines to detect unauthorized access to applications. The software reports its findings to the Configuration Control Board, which is able to automatically and remotely delete the compromised applications. The software, Triumphant’s Resolution Manager, uses recognition filters to monitor application access. The Board meets every week to review flagged software and offer users the opportunity to defend their access to applications which are not yet authorized.

<http://www.networkworld.com/news/2008/10/0708-army-desktop-software.html?fsrc=netflash-rss>

### **New command coming to Ft. Gordon**

FORT GORDON PUBLIC AFFAIRS OFFICE  
10/15/2008

The U.S. Army has announced that the 7th Theater Signal Command will have headquarters at Fort Gordon, GA, and that Brigadier General Jennifer Napper will serve as commander. The mission of the Command is to defend the Continental U.S. portion of LandWarNet, the Army’s global computer network. The 93rd Signal Brigade, which was at Fort Gordon, will be activated at Fort Eustis, VA.



The 106th Signal Brigade, part of the 7th Signal Command which was also formerly located at Fort Gordon, will be activated at Fort Sam Houston, TX.

<http://www.wrdw.com/home/headlines/31001079.html>

### **HSPD-12 card may promote information sharing**

BY: MARY MOSQUERA, FEDERAL COMPUTER WEEK  
10/09/2008

Dave Wennergren, deputy chief information officer at the Defense Department, states that once agencies issue personal identification cards to federal employees, they will be able to look into other uses for the cards. Under Homeland Security Presidential Directive 12, the cards will provide identity authentication in an effort to improve physical and logical security across the government. Card readers are also able to detect fraudulent cards from embedded information. The DoD hopes the cards will be able to improve information sharing and trust.

<http://www.fcw.com/online/news/154042-1.html>

### **USAF Cyber Command Whittling Down List of Possible Bases**

BY: BETTINA H. CHAVANNE, AEROSPACE DAILY & DEFENSE REPORT  
10/20/2008

Maj. Gen. William Lord states the Air Force will be evaluating the 56 possible headquarter bases for U.S. Air Force Cyber Command over the next few months. Lord also explains that the decision to designate the Cyber Command as a Numbered Air Force under U.S. Air Force Space Command. Lord also discusses the many similarities between the Air Force Cyber mission and the other domains, including the coordinated use of kinetic and non-kinetic weapons.

### **Shelton: Integrate Space and Cyber Ops**

BY: GAYLE PUTRICH, DEFENSE NEWS  
10/08/2008

Lt. Gen. Willaim Shelton, commander of the 14th Air Force and U.S. Strategic Command's Joint Functional Component Command for Space, spoke at the Space Foundation's annual defense-centered conference, stating that space and cyberspace operations must get closer in order for the Department of Defense to get the most out of both domains. During the panel discussion, Shelton said that space capabilities must be truly joint and a change in the traditional view of combat is needed for the advancement of both space and cyberspace. Shelton said that both domains are "inherently global" and must be integrated.

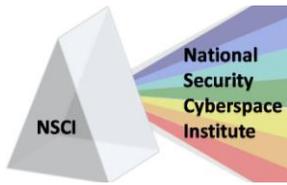
<http://www.defensenews.com/story.php?i=3762587>

### **Air Force demotes Cyberspace Command**

BY: KEVIN FOGARTY, DEFENSE SYSTEMS  
10/13/2008

After a series of meetings in Colorado Springs, Colo., the Air Force announced that the provisional Cyberspace Command would not a major Air Force command like the Air Combat or Space commands. The cyberspace initiative will instead be part of the numbered Air Force as part of Space Command, in the hopes of integrating cyberspace into the mission to secure the exploitation of space. John Pike, director of GlobalSecurity.org explains that the move makes sense because cyberspace and space share common elements including control and communication of information, and also said that details of the reorganization will most likely come after the presidential election.

<http://defensesystems.com/Articles/2008/10/Air-Force-demotes-Cyberspace-Command.aspx>



### **OP-ED: Cyber is bigger than Barksdale**

SHREVEPORT TIMES (LA.)  
10/14/2008

The Air Force has announced that it will not create a separate Cyber Command, but Barksdale Air Force Base will still receive educational and commercial opportunities in cybersecurity. Despite the announcement, Louisiana may still be well positioned in the cyberworld, evidenced by the 700 attendees from industry, academia and the military that met in Shreveport to discuss cyber security, cyber infrastructure and education. The Air Force will still decide on a place to base the military's cyber efforts that will be part of a numbered Air Force, and the state has worked to bring capabilities to state universities for cyber research.

### **Cyber change is 'streamlining'**

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

Maj. Gen. William T. Lord spoke to media following his talk at the Cyber Awareness Summit in Shreveport, LA., and said that the changes in the Air Force Cyber Command may benefit Barksdale Air Force Base, the headquarters of the provisional Command. Lord and Democratic Senator Mary Landrieu agree that there are still many opportunities for Barksdale for future cyber missions. Bossier City Mayor Lo Walker, who also spoke at the Summit, states the city's decision to contribute a significant amount to the \$107 million Cyber Innovation Center was a good investment, and that cyber opportunities are broader than just the military.

<http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20081010/NEWS01/810100329&referrer=FRONTPAGECAROUSEL>

## **CYBERSPACE LESSONS LEARNED**

### **Lessons Learned From Cyber Storm II**

CONTINUITY CENTRAL  
09/25/2008

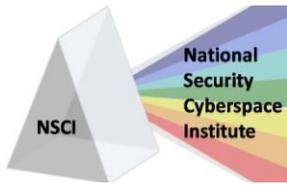
Cyber Storm II was an exercise held by the U.S. Department of Homeland Security, which brought together government and industry from Australia, Canada, New Zealand, the United Kingdom and the United States to test and analyze cybersecurity arrangements. The Cyber Storm II national cyber security exercise final report has been released. The article lists

key findings contained in the report, including: response is enhanced by testing standard operating procedures and crisis management plans; interaction among key players enhanced effective response during an incident; crisis response to a cyber incident must also take into consideration multiple interdependencies.

<http://www.continuitycentral.com/news04174.html>



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.



### **Security Lessons from the World Bank Breach**

BY: JOAN GOODCHILD, CSO  
10/14/2008

Recent reports announced that servers at the World Bank Group have been compromised and breached multiple times within the last year. Details are unavailable, but the report claims there were six major network intrusions including unauthorized access to the bank's network in June and July 2008, although officials with the World Bank are claiming there are errors in the report from Fox News. Graham

Culey, senior technology consultant with IT security firm Sophos, states that there are lessons that companies can learn from the breaches regardless of allegations which include: no one is completely safe from cyber thieves; motivation for attacks can be financial or political; even large companies are vulnerable; and we are still addressing the basics of security failures which lead to major breaches. Each of these are discussed in detail in the article.

[http://www.csoonline.com/article/454675/ Security Lessons From the World Bank Breach](http://www.csoonline.com/article/454675/Security%20Lessons%20From%20the%20World%20Bank%20Breach)

## **CYBERSPACE RESEARCH: FINDINGS AND OPPORTUNITIES**

### **Buzz of the Week: Hopes for cybersecurity**

FEDERAL COMPUTER WEEK  
10/20/2008

The Federal Government announced the new Leap Year Program, which will provide money to industry for research and development into emerging security technologies, as part of the Comprehensive National Cybersecurity Initiative. DHS hopes that the program will bring significant technological advances which will result in widely available commercial products. Still, some fear the program may not be realistic, and could suffer from "bad governance, poor investments or just a dearth of good ideas."

[http://www.fcw.com/print/22\\_34/news/154078-1.html?page=1](http://www.fcw.com/print/22_34/news/154078-1.html?page=1)

(CNCI). Specifically, DHS will be looking for new services and reexamining old services for help with implementing new analytics and operations. Michael Brown, DHS' deputy assistant secretary for cybersecurity and communications, explained that once the program is approved, DHS will be able to disclose more specific details to vendors and also acknowledged the enormous interest from industry regarding the initiative. The National Science Foundation, a part of the CNCI, has requested information in regards to potential cybersecurity technology.

<http://www.fcw.com/online/news/154103-1.html>

### **DHS to hold industry day on cyber initiative**

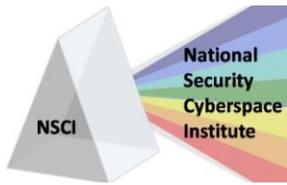
BY: BEN BAIN, FEDERAL COMPUTER WEEK  
10/16/2008

The Homeland Security Department is planning to hold a vendor day this December or January exclusively for cybersecurity and communications organizations in order to provide contractors with details from the Comprehensive National Cybersecurity Initiative

### **Government Awards Contract for Cyber-Behavior Research**

BY: DREW CONWAY, NYU BLOGS  
10/10/2008

A research program from ODNI proposed investigation into how a person's online behavior could impact their application for a security clearance. FBO has announced that the research, with a combined value of over \$800,000, will be awarded to the Syracuse Research Corporation and the Personnel



Decisions Research Institutes. Neither group has currently issued an official press release.

[http://blogs.nyu.edu/blogs/agc282/zia/2008/10/government\\_awards\\_contract\\_for.html](http://blogs.nyu.edu/blogs/agc282/zia/2008/10/government_awards_contract_for.html)

### **Air Force lab issues long-term BAA for cyber defense research**

DEFENSE DAILY

10/15/2008

The Air Force Research Laboratory has issued a Broad Agency Announcement (BAA) for research proposals in six areas related to cyber defense which are: Strategic Cyber Defense;

Global Cyber Situational Understanding; Incorruptible Date Codes and Executables; Cybercraft; Assured Load Balancing Enterprise; and Self Regenerating Incorruptible Enterprise.

The Air Force hopes to develop a system to avoid threats and deter attacks, as well as improve situational awareness using new technologies. There is \$49.9 million available under the BAA, and awards will range in value from \$100,000 to \$1 million annually. Initial proposals are due by December 1, 2008.

<http://www.defensedaily.com/publications/dd/4356.html>

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

ITT

### **Cellphone Botnets, Blackmailing VOIP & a Healthy Cybercrime Economy**

BY: KELLY JACKSON HIGGINS, DARK READING

10/15/2008

According to research by the Georgia Tech Information Security Center, about 15% of all computers online are infected bots, which is a 5% increase from last year. The Center reported on recent research findings at the GTISC Security Summit on Emerging Cyber Security Threats. Among the findings, Wenke Lee, a botnet researcher, believes that the next trend in cybercrime will be an increase in recruitment of cell phones and PDAs as botnets. This is especially dangerous because an army of cell phone botnets could attack the wireless infrastructure. The article discusses additional trends in cybercrime, including an increase of

cyber warfare used in coordination with traditional warfare.

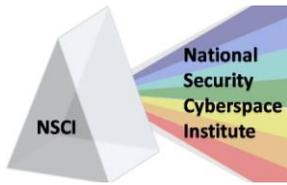
[http://www.darkreading.com/document.asp?doc\\_id=166029&WT.svl=news1\\_1](http://www.darkreading.com/document.asp?doc_id=166029&WT.svl=news1_1)

### **DISA seeks state-of-the-art security assessment services**

BY: DOUG BEIZER, FEDERAL COMPUTER WEEK

10/07/2008

The Defense Information Systems Agency has requested information on new technologies for securing Defense Department networks. The article describes the three necessary functions of the Assured Compliance Assessment Solution which are: ensuring compliance with current DoD standards and practices; the ability to scan software, hardware and system configurations



for vulnerabilities; and the provision of network situational awareness.

<http://www.fcw.com/online/news/154018-1.html>

### **Users, Enterprises Pay for Poor Privacy Policies, Study Says**

BY: TIM WILSON, DARK READING

10/07/2008

A research report by Carnegie Mellon University researchers Aleecia McDonald and Lorrie Faith Cranor addresses the privacy policy issues that are affecting cybersecurity. The researchers explain the current policies are lengthy, poorly written and too complex, causing most Internet users to have a poor understanding of privacy risks on many Web sites. The report measured the time required to review Web site privacy policies and assigned a monetary value to the time users would need to review the policies adequately. Although some feel the figures are “contrived”, the research still proves that the complexity and length of policies are intimidating to many users and recommends businesses streamline the policies. The paper also suggests that there may be a need for legal standards for Internet privacy policies.

[http://www.darkreading.com/document.asp?doc\\_id=165411](http://www.darkreading.com/document.asp?doc_id=165411)

### **Security Software Suites No Match for Custom Attacks**

BY: BRIAN KREBS, WASHINGTON POST

10/13/2008

Security analysis firm Secunia tested a dozen security suites for effectiveness against malware and direct attacks to more than 150 software flaws, and found that even the major anti-virus vendors fail at detecting malware aimed at the vulnerabilities. The vulnerabilities were all publicly detailed in the Common Vulnerabilities and Exposures (CVE) database or found in software updates from program makers. 126 of the 300 test cases would affect

popular products, and testing found that even popular vendors such as McAfee, Microsoft and TrendMicro only detected between one and three percent of the attacks. Some argue that the study ignores the reality of current threats because almost none rely on software vulnerabilities, but rather tricking users into installing malicious software.

[http://voices.washingtonpost.com/securityfix/2008/10/security\\_software\\_suites\\_vs\\_cu.html?nav=rss\\_blog](http://voices.washingtonpost.com/securityfix/2008/10/security_software_suites_vs_cu.html?nav=rss_blog)

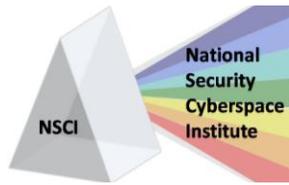
### **Botnet experts meet as threat grows for corporations**

BY: DAN KAPLAN, SC MAGAZINE

10/21/2008

200 security researchers including law enforcement officers and academics met at the International Botnet Task Force in Arlington, VA. The group meets twice a year to share information and case studies. Researchers discussed the increasing threat of botnet attacks, which are of particular concern for large corporations because infected machines could hold personal information or important research. Botnets are especially dangerous because they can spread extremely quickly, and are often part of downloads. Victims are not aware that their computers are becoming infected, and most security software does not detect the infection. Researchers discussed the issue of liability and whether a corporation should be held accountable if their infected computers are part of a DoS attack. Researchers also stated that banks have the most to lose from botnets, because they could be liable for infecting customer's computers.

<http://www.scmagazineus.com/Botnet-experts-meet-as-threat-grows-for-corporations/article/119773/>



### **Report: Energy Companies Are Top Target of Web-Borne Malware**

BY: KELLY JACKSON HIGGINS, DARK READING  
10/21/2008

According to the "Global Threat Report" from ScanSafe, energy companies have experienced more malware attacks in this year's third quarter than any other vertical market with an increased rate of exposure of 189 percent. The report also states that overall, corporations experienced a 338 percent increase in Web-based malware exposure versus the first quarter of this year. Backdoor and password-stealing Trojans are the types of malware increasing the most.

[http://www.darkreading.com/document.asp?doc\\_id=166407](http://www.darkreading.com/document.asp?doc_id=166407)

### **Up next: Cellular botnets, cybermilitias**

BY: JAIKUMAR VIJAYAN, COMPUTER WORLD  
10/17/2008

According to a recent report by the Georgia Tech Information Security Center (GTISC), malware writers will continue to advance faster than the security industry. The report explains that a major concern for cyber security in the near future will be smart phones, which are increasingly operating more like traditional PC environments. This is an important emerging security threat because cell phones and PDA devices are often not secured even as minimally as most PCs. The article also discusses the threat of cyber militias and increasingly effective botnets.

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117424&source=rss\\_topic82](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117424&source=rss_topic82)

### **Georgian cyberattacks suggest Russian involvement, say researchers**

BY: GREGG KEIZER, COMPUTER WORLD  
10/17/2008

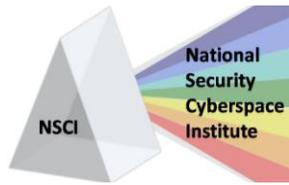
A volunteer group of computer security and intelligence experts, called Project Grey Goose", recently investigated links between Russian government Web sites and the cyber attacks against Georgian government sites. Principal investigator Jeff Carr explains that there were organized target lists and postings on sites such as StopGeorgia.ru which corresponded to attacks on the Georgian Web sites. According to Carr, as well as the group's report, there was some communication between the Russian government and "leaders" who distributed hacking tools and instructions to a number of novice hackers who carried out the attacks. The report also claims that the type of attacks carried out would have required much preparation long before the actual conflict.

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117439&source=rss\\_topic82](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117439&source=rss_topic82)

### **Report: Russian Hacker Forums Fueled Georgia Cyber Attacks**

BY: BRIAN KREBS, WASHINGTON POST  
10/16/2008

Experts from Project Grey Goose, a group of more than 100 security experts, claim that while exhaustive research into the August cyber attacks against Estonia cannot prove involvement of the Russian government, there is still evidence that Russian officials at the least did not discourage the online assault. The report released by the group states that the attacks were coordinated from a Russian Web site forum which was equipped with target lists and vulnerability details well before the conflict. At one of these forums, StopGeorgia.ru, the researchers found target lists and detailed instructions which enabled inexperienced hackers to carry out attacks. Jeff Carr, a lead



investigator, believes that the Russian government may be offering its support to these hacker groups, but attacks are not directly coordinated by the Russian government, allowing government officials to deny responsibility of the attacks.

[http://voices.washingtonpost.com/securityfix/2008/10/report\\_russian\\_hacker\\_forums\\_f.html?nav=rss\\_blog](http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html?nav=rss_blog)

### **Spies Launch 'Cyber-Behavior' Investigation**

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK  
10/12/2008

The Office of the Director of National Intelligence (ODNI) has awarded \$800,000 to researchers to investigate the cyber behavior of individual's applying for security clearances. Qualifying "online behavior" would include social network usage, compulsive internet use, material distribution, and contact with foreign nationals. The ODNI will also define what is considered normal or acceptable online behavior.

<http://blog.wired.com/defense/2008/10/spies-launch-cy.html>

### **Study: 80% of Organizations Suffer Breaches, Most From the Inside**

BY: KELLY JACKSON HIGGINS, DARK READING  
10/09/2008

A study by the Ponemon Institute found that 75% of organizations in the United States, United Kingdom, France and Germany have been victims of data breaches caused by accidental internal lapses, and 26% have experienced breaches by malicious insiders. The Institute surveyed more than 1,000 IT professionals in the United States, and found that there is an increase in breaches caused by insiders, both accidentally and purposefully, which have resulted in leaked or stolen data. Most breaches originate from mobile devices such as laptops, PDAs and memory sticks. Only 5% of the respondents said that they notify victims "almost immediately" after detecting a data breach.

[http://www.darkreading.com/document.asp?doc\\_id=165612](http://www.darkreading.com/document.asp?doc_id=165612)

## **CYBERSPACE HACKS, TACTICS AND DEFENSE**

### **Report: U.S. not prepared for EMP attacks**

BY: ALICE LIPOWICZ, FEDERAL COMPUTER WEEK  
10/22/2008

The Heritage Foundation has released a report stating the threat of a electromagnetic pulse attack, which could cause significant economic damage by disabling computer systems, power grids and communications, has not seen much attention by Congress or President Bush. The report also claims that the Homeland Security Department has yet to address the threat of EMP attacks that were included in the National Infrastructure Protection Plan. The report also included recommendations for the new administration including more investment in research which must evaluate the risks and likelihood of EMP attacks.

<http://www.fcw.com/online/news/154155-1.html>

### **Cyber-attack theory as al-Qaida websites close**

BY: IAN BLACK, THE GUARDIAN  
10/22/2008

Three al-Qaida propaganda Web Sites, al-Ekhlal, al-Buraq, and al-Firdaws were all shut down following the delay of the annual September 11 propaganda video. One of the sites, al-Fajr claims that technical problems have caused the disruption in service and that the sites have not been victims of enemy hackers, although many experts believe Saudi intelligence is responsible. Some researchers,



## Keeping Cyberspace Professionals Informed

such as those at the Gulf Research Centre in Dubai, believe that Shia and Sunni groups have both been involved in cyberattacks against the other; others, such as Norway's Defence Research Establishment, believe that the size of the attacks signify the involvement of a government intelligence agency. Another theory claims that al-Qaida shut down the sites to prevent enemies from having access to the information.

<http://www.guardian.co.uk/world/2008/oct/22/alqaida-terrorism-internet>

### **IG says Defense systems lack reliable safeguards against hackers**

BY: BOB BREWIN, NEXTGOV  
10/09/2008

The Defense Department inspector general released a report claiming the Defense

Information System Agency's computing centers lack the capability to detect suspicious activity, unauthorized access, and attempts to disable the agency's computer systems. The data centers use records of computer events to monitor activity, but the IG report states there are not adequate procedures for monitoring access and suspected security violations. The IG recommended new software audit capabilities, and DISA officials responded by saying the agency does not currently have the tools to satisfy the IG recommendations.

[http://www.nextgov.com/nextgov/ng\\_20081009\\_8610.php](http://www.nextgov.com/nextgov/ng_20081009_8610.php)

## CISCO SYSTEMS

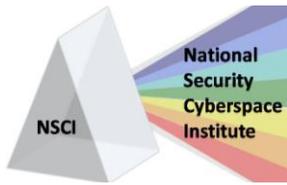


### **CISCO**

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)



### **FTC warns consumers of increase in Internet scams**

OAKLAND PRESS  
10/09/2008

The Federal Trade Commission warned that phishing e-mail scams that steal personal data may have an impact on the current financial crisis. The FTC claims that hackers are taking advantage of the crisis by sending spam e-mails from fake bank or mortgage companies, which victims are more likely to believe are legitimate. The FTC also warns that the emails may request information such as account numbers, passwords, or social security numbers, which most banks and financial institutions would never request. The article also provides the link for the FTC guide for consumers to educate themselves about these types of scams.

<http://www.theoaklandpress.com/articles/2008/10/09/business/doc48ee5464af1b0135101446.txt>

### **Organized cybercrime replaces random individual attacks**

NET SECURITY  
10/15/2008

The Information Security Forum claims that organized, profit-driven attacks are replacing the small scale hacks of the past, which presents increased threats for both industry and the government. Most of these attacks are aimed at collecting valuable or sensitive information or customer data for financial gain. The article discusses the five "phases" of a profit-driven attack, and profiles the usual targets of these attacks. The article also states that cybercrime is the fastest growing type of crime and the U.S. Treasury has claimed that cybercrime has exceeded the profits of illicit drug sales.

<http://www.net-security.org/secworld.php?id=6646&MENU>

### **Managing Mercenaries**

STRATEGY PAGE  
10/21/2008

The U.S. FBI states 24 nations have developed offensive cyber capabilities, including hacker tools and techniques, usually as part of improvements to their own infrastructure defense. The FBI claims Internet criminal gangs may provide some nations with offensive tools, and is working to better track these criminal gangs. Although there are cases of criminal gang involvement in cyber attacks and espionage, the FBI explains most nations still regard the groups as dangerous criminals.

<http://www.strategypage.com/htmw/htiw/articles/20081021.aspx>

### **NEFA Foundation: Al-Fajr Center Announces Shuttering of Three Top Jihad Web Forums**

BY: EVAN KOHLMANN, COUNTERTERRORISM BLOG  
10/11/2008

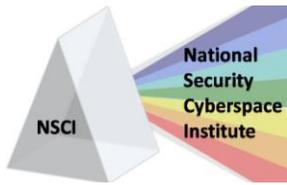
A statement issued by the Al-Fajr Media Center announced that the closure of three Internet forums used by Al-Qaida were due to technical reasons and not because of attacks from "the hands of the enemy" as was previously reported. The statement also said that the three forums, Al-Ekhlaas, Al-Firdaws, and Al-Boraq will likely be available online for some time, but that users should be careful to avoid links from sources other than those officially announced by the Al-Fajr Media Center.

[http://counterterrorismblog.org/2008/10/nefa\\_foundation\\_alfajr\\_center.php](http://counterterrorismblog.org/2008/10/nefa_foundation_alfajr_center.php)

### **New USAF weapon could shut down or damage enemy electronics**

BY: DAVID A. FULGHUM AND AMY BUTLER,  
AVIATION WEEK & SPACE TECHNOLOGY  
10/20/2008

According to officials at Eglin AFB, Fla., the Air Force Research Laboratory is developing an "airborne, electronics-killing, standoff weapon"



system that will generate pulses of high-power microwaves. The program could receive funding for feasibility studies and flight-testing in the Fiscal 2010 budget. The weapons system, called "Champ", would also be part of an analysis of alternative weapons systems that will start in 2012 in an effort to find the most effective weapons solution. The "Champ" system would target enemy air defenses, command-and-control centers, radars, communications, mobile missiles and airfields.

### **Microsoft under threat from new attack code**

BY: ROBERT MCMILLAN, IDG NEWS SERVICE  
10/17/2008

Microsoft has released a patch for a security flaw that is part of the Metasploit hacking toolkit, which could affect Microsoft's Host Integration Server 2006. Russ Cooper, a manager with Verizon Business's RISK Team, explains that normally users would be required to have an account to access the Host Integration Server, but vulnerabilities in machines such as test systems could allow malware in. Microsoft has patched 20 security flaws this month, although this particular flaw was the only one that has been exploited by hackers since the patches were released.  
<http://www.techworld.com/news/index.cfm?RSS&NewsID=105844>

### **Warezov botnet rises from the grave**

BY: DAN GOODIN, THE REGISTER  
10/16/2008

Joe Stewart, director of malware research at SecureWorks, states that the Trojan programs which install the Warezov bot are back on websites such as those offering free MP3s, although the attacks are different than the email attachment attacks that from 2006. Warezov is more like a "payload delivery system" according to Stewart because of the malware's ability to install any software the

operator wants from a master server. The return of the Warezov botnet comes as a surprise to some security experts given the recent defeat of the Storm botnet and success of U.S. law enforcement against spam gangs.  
[http://www.theregister.co.uk/2008/10/16/warezovs\\_second\\_coming/](http://www.theregister.co.uk/2008/10/16/warezovs_second_coming/)

### **NY tops computer virus threat list**

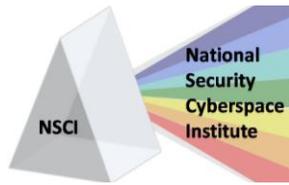
MX LOGIC  
10/01/2008

Security software firm, PC tools, has released research which found that New York is at the top of a list of most at-risk cities in the United States. The top five also included Houston, Los Angeles, Chicago, and Miami. Spokesperson Michael Greene states most attacks are from spyware, adware, viruses and keyloggers. The report also identified the top vulnerabilities for Windows users such as a lack of adequate virus protection.  
<http://www.mxlogic.com/securitynews/viruses-worms/ny-tops-computer-virus-threat-list682.cfm>

### **Third-Party Hack**

BY: JOHN H. SAWYER, DARK READING  
10/06/2008

Kris Harms from Mandiant states most companies are unaware of data breaches until they are notified through a third party. Author, John H. Sawyer, discusses the possibility that businesses could be liable for damages resulting from data breaches from compromised servers that were used to attack another company. Even if a company is unaware of a data breach or compromised server, Sawyer wonders if the company would still be held responsible or face lawsuits and bad publicity.  
[http://www.darkreading.com/blog.asp?blog\\_sectionid=447](http://www.darkreading.com/blog.asp?blog_sectionid=447)



### **Free Tool Hacks Banking, Webmail, and Social Networking Sessions**

BY: KELLY JACKSON HIGGINS, DARK READING  
10/06/2008

Researcher Jay Beale demonstrated the “Middler” open-source tool at the SecTor conference in Toronto. The “plug-and-play hacking tool” is able to generate attacks on online banking and social networking sites despite secure login processes or SSL protections by cloning a user’s online session with cookies and HTML form parameters from the victim. The tool loads malicious JavaScript onto the sites, and is dangerous because hackers with no experience to easily develop attacks. Beale will also demonstrate how Middler can affect software installations; inject Trojan viruses; and how the tool can work with the Metasploit hacking tool to launch cross-site forgery attacks.

[http://www.darkreading.com/document.asp?doc\\_id=165303](http://www.darkreading.com/document.asp?doc_id=165303)

### **Storm May Finally Be Over**

DARK READING  
10/13/2008

Botnet researchers believe the month of inactivity from the Storm botnet may signify the end of the spam run. Joe Stewart, director of malware research for SecureWorks explains that prolonged inactivity often means that operators have abandoned a bot, and also states that the Storm botnet has been active since it started with major spam campaigns. Paul Royal, director of research for Damballa, explains that the botnet is currently ten times smaller than it was just months ago, and that it is unlikely that the botnet would be very powerful even if it was reinvented now. Researchers believe the large amount of attention from researchers and press that massive botnets such as Storm and Kraken

attract makes it difficult to efficiently operate for long.

[http://www.darkreading.com/document.asp?doc\\_id=165798&f\\_src=darkreading\\_default](http://www.darkreading.com/document.asp?doc_id=165798&f_src=darkreading_default)

### **Hackers force Al-Arabiya site name change**

BY: IAN BLACK, THE GUARDIAN  
10/13/2008

Al-Arabiya Television has been forced to change its internet domain name after it was victim to a cyber attack by “organized extremists”.

Although no one has claimed responsibility, al-Arabiya is associated with the Sunni group, and the hacked website showed pictures of a burning Israeli flag with the caption, “Serious warning: If attacks on Shia websites continue, none of your websites will be safe”. Someone who claimed to be the hacker emailed Gulf News claiming that al-Arabia wanted to start a war with Shia Muslims. The attack has since sparked debates on Arab Web sites.

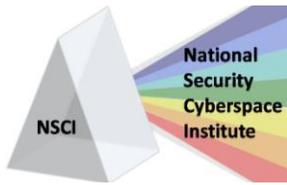
<http://www.guardian.co.uk/world/2008/oct/13/middleeast-internet>

### **Saudi-owned TV website hit by cyber attack (AFP)**

YAHOO! TECH NEWS  
10/10/2008

Hackers, who claim to be Shiite, attacked the Saudi-owned Al-Arabiya website, and posted a message that said, “If attacks on Shiite websites continue, none of your websites will be safe” and a picture of a burning Israeli flag. Iranian news has recently reported that Wahhabi hackers have attacked more than 300 Shiite websites. Al-Arabiya issued a statement saying that they had been attacked by organized extremists and that they will remain moderate and objective.

[http://tech.yahoo.com/news/afp/20081010/tc\\_afp/uaereligioninternetmediasaudi](http://tech.yahoo.com/news/afp/20081010/tc_afp/uaereligioninternetmediasaudi)



### 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.

#### 10,000 LinkedIn users targeted in spear phishing attack

BY: ANGELA MOSCARITOLLO, SC MAGAZINE  
10/09/2008

A recent email scam which tricked victims into downloading malicious software targeted ten thousand users of LinkedIn, a social networking site for professional networking. The emails addressed recipients by name, and had a subject line reading "Re: business contact" which made the email appear to be authentic. The email contained an attachment which was said to be a list of business contacts that were requested by the recipients, but was actually malicious software which stole usernames and passwords from the victim. Hackers gain access to databases of information including names, emails and identifying information on the victims, which can make a phishing email seem legitimate.

<http://www.scmagazineus.com/10000-LinkedIn-users-targeted-in-spear-phishing-attack/article/119268/>

#### Metasploit 3.2 Offers More 'Evil Deeds'

BY: SEAN MICHAEL KERNER, INTERNET NEWS  
10/08/2008

Metasploit create H.D. Moore discussed details of the new features in the Metasploit 3.2 release at the SecTor conference in Toronto. Metasploit, which is an "open source attack framework" developed in 2003, will now feature a context map payload feature, which will make detecting attack code more difficult.

Other new features include support for exploiting multi-core CPU machines, and a "super weapon that will make exploiting browsers a trivial matter". Moore also said the new Evil Wireless Access Point feature allows the creation of access points and spoofing of access points on user's preferred lists, and announced that Metasploit 3.2 will have full IPv6 support.

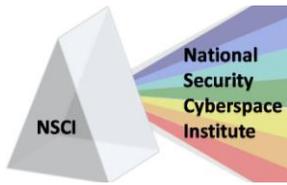
<http://www.internetnews.com/dev-news/article.php/3776831/Metasploit+32+Offers+More+Evil+Deeds.htm>

#### Skype Acknowledges Chinese Spying

BY: MARK HACHMAN, PC MAGAZINE  
10/03/2008

Skype President Tom Silverman announced that Chinese users have had instant messages blocked and copied to other servers that are owned by Skype's partner, TOM Online. Silverman explained that he was aware when Skype partnered with Tom that Tom would censor messages with certain keywords, as authorized by the Chinese government. Silverman said that he was not aware that Tom would store the messages on its servers, which resulted in many of the messages being stolen by a third party which gained unauthorized access. Some believe the Chinese government is monitoring the communications.

<http://www.pcmag.com/article2/0,2817,2331756,00.asp>



## CYBERSPACE – LEGAL

### **FBI says Dark Market sting netted 56 arrests**

BY: ROBERT MCMILLAN, COMPUTER WORLD  
10/16/2008

The FBI recently reported that the two-year undercover operation on the DarkMarket.ws Web site resulted in the arrest of 56 cyber criminals, and also prevented significant economic losses. The Web site, which had more than 2,500 members before it was shut down this month, is used by criminals to buy and sell stolen personal information including credit card numbers. The FBI worked with authorities in the U.K., Turkey, and Germany. The FBI reports the confiscation of compromised accounts and information prevented about \$70 million in fraud.

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117361&source=rss\\_topic82](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117361&source=rss_topic82)

### **Student gets jail for crashing university servers**

BY: ROBERT MCMILLAN, COMPUTERWORLD  
10/22/2008

Ryan Goldstein, a student at the University of Pennsylvania, was arrested as part of the FBI's "Operation Bot Roast II" and has been sentenced to three months in prison for involvement in distributed denial-of-service attacks against the University in 2006. Goldstein was also fined \$30,000 and \$6,100 in restitution to the University. Owen Walker, a New Zealand hacker, helped to launch the attacks with Goldstein, but was given no prison time because of the differences in United States and New Zealand laws. Authorities reported that Goldstein provided Walker with log-in information and malicious hacking software in exchange for help with launching the attack.

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117811&source=rss\\_topic82](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117811&source=rss_topic82)

### **Opinion: FTC's New Red Flag Rules cast wide identity theft net**

BY: JEROME WENDT, COMPUTERWORLD  
10/15/2008

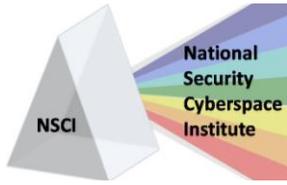
In addition to numerous rules and regulations already observed by most corporations, the Federal Trade Commission will now require compliance with their Red Flag Rules, which previously applied mainly to the financial industry, which maintains large amounts of personal information. The Red Flag Rules are designed to prevent phishing attacks by requiring corporations to implement programs which detect and prevent identity theft. The FTC has recently made all redefined terms of the rules, which means that any corporation that extends or renews credit to its customers will be required to comply.

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=&articleId=9117223&taxonomyId=&intsrc=kc\\_feat](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=&articleId=9117223&taxonomyId=&intsrc=kc_feat)

### **German court says IP addresses in server logs are not personal data**

OUT-LAW NEWS  
10/14/2008

German courts have ruled that storing internet protocol (IP) addresses of visitors does not violate current data protection laws because they are not considered personal data. Privacy activists argue IP addresses should be considered personal data because they can potentially identify the user's identity, however, the court said an internet service provider could not identify a user by an IP address without legal basis unless the information was illegally



transferred to a third party. Web sites such as search engines and publishing operations use IP addresses to identify users and their online habits. The UK's Information Commissioner has published guidance stating that IP addresses are not personal data because of the difficulty of using IP addresses to build an actual user profile.

<http://www.out-law.com/page-9505>

### **Intellectual Property Bill Becomes Law: Critics Say It Goes Too Far**

BY: TIM WILSON, DARK READING  
10/14/2008

President Bush has signed the Prioritizing Resources and Organization for Intellectual

Property Act (PRO-IP) which will toughen laws on theft of intellectual property and also appoints a new cabinet position to oversee the IP infringement effort. The bill will steepen legal penalties as well as increase Department of Justice resources for coordinating counterfeiting and piracy efforts among state and federal government. Critics claim that the harsher penalties give too much discretion to prosecutors in complex IP and IT cases. President Bush, who originally opposed the bill, signed it after a provision giving the DoJ the right to pursue civil litigation against copyright infringers was removed.

[http://www.darkreading.com/document.asp?doc\\_id=165924](http://www.darkreading.com/document.asp?doc_id=165924)

## **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](#).

28-30 Oct 2008	<b>International Conference on Risks and Security of Internet Systems</b> , Tozeur Turkey, <a href="http://www.redcad.org/crisis2008/">http://www.redcad.org/crisis2008/</a>
3-5 Nov 2008	<b>Global MilSatCom 2008 Conference &amp; Exhibition</b> , Millennium Conference Centre, London, UK, <a href="http://www.smi-online.co.uk/08globalmilsatcom20.asp">www.smi-online.co.uk/08globalmilsatcom20.asp</a>
3-4 Dec 2008	<b>FinSEc 2008</b> , Palm Beach Gardens FL, <a href="http://www.misti.com/default.asp?page=65&amp;Return=70&amp;ProductID=7474">http://www.misti.com/default.asp?page=65&amp;Return=70&amp;ProductID=7474</a>
11-12 Dec 2008	<b>European Conference on Computer Network Defense</b> , Dublin Ireland, <a href="http://2008.ec2nd.org/ec2nd/597-EE.html">http://2008.ec2nd.org/ec2nd/597-EE.html</a>
19-21 Jan 2009	<b>International Workshop on e-Forensics Law</b> , Adelaide Australia, <a href="http://www.e-forensics.eu/">http://www.e-forensics.eu/</a>
26-29 Jan 2009	<b>U.S. Department of Defense Cyber Crime Conference</b> , St Louis MO, <a href="http://www.dodcybercrime.com/9CC/">http://www.dodcybercrime.com/9CC/</a>
16-19 Feb 2009	<b>Black Hat DC 2009</b> , Washington DC, <a href="http://www.blackhat.com/">http://www.blackhat.com/</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>
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>
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>
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>

