



# CyberPro

Volume 2, Edition 19  
September 24, 2009

## Keeping Cyberspace Professionals Informed

<p style="text-align: center;"><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>-----</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 style="text-align: center;">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 CyberPro may not be published, broadcast, rewritten or redistributed without prior NSCI consent.**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

<b>This Week in CyberPro</b> .....	<b>5</b>
<b>Senior Leader Perspective: RADM Elizabeth Hight</b> .....	<b>6</b>
<b>Cyberspace – Big Picture</b> .....	<b>12</b>
The Five Most Dangerous Internet Security Myths .....	12
There’s Concern, But Where’s the Action? .....	12
<b>Cyberspace – U.S. Government</b> .....	<b>13</b>
FCC Chair Proposes ‘Open Internet’ Rules.....	13
FCC Chairman Expected to Outline Net Neutrality Rules .....	13
Feds Can Monitor Personal E-Mail Sent Privately to Gov’t Workers, DOJ Says .....	13
Intell Agencies Plan to Beef Up Cybersecurity .....	13
Committee Examines Growing Cyber Threat to Businesses .....	14
Government Should Help Widen Cyber Knowledge.....	14
Cyber Criminals Targeting Small Businesses .....	15
Republican Lawmakers Want Answers from ICANN.....	15
<b>U.S. Cyber Leadership Debate</b> .....	<b>16</b>
Pressure Builds on Obama to Appoint Cybersecurity Coordinator .....	16
Gates: No New Cyber-Eavesdropping Agency .....	16
<b>Cyberspace – Department of Defense (DoD)</b> .....	<b>16</b>
Balancing Social Networking and Cybersecurity .....	16
Cyber Threat Calls for Flexibility in Command Model, General Says .....	16
John Arquilla: Go on the Cyberoffensive .....	17
<b>Cyberspace – Department of Homeland Security (DHS)</b> .....	<b>17</b>
Authentication Said Key to Cybersecurity .....	17
Homeland Security to More Than Double Staff for Cyber Threats.....	17
Testimony: Hackers Better Organized than Government.....	18
<b>Cyberspace – International</b> .....	<b>19</b>
How is Government Coping with Cyber Crime? .....	19
MI5 Ropes in Teenage Hackers to Combat Cyber Terrorism .....	19
South Korea to Train 2,000 ‘Cyber Sheriffs:’ Report .....	19
The South Asian Cyber War Threat .....	20



# CyberPro

Volume 2, Edition 19  
September 24, 2009

## Keeping Cyberspace Professionals Informed

<b>Cyberspace Research .....</b>	<b>20</b>
Researchers Overwhelming Vendors with Security Flaws .....	20
Microsoft Internet Explorer SSL Security Hole Lingers .....	21
Snow Leopard Less Secure than Windows, Says Hacker .....	21
Botnet PCs Stay Infected for Years .....	21
The Internet is the new Wild West, reports IBM Consultant .....	21
Phishing Attacks Fell by 45% in August .....	22
<b>Cyberspace Hacks and Attacks .....</b>	<b>22</b>
New York Times Scareware Attack Shows Weakness of Ad Networks .....	22
Steganography Meets VoIP in Hacker World .....	23
Zeus Internet Banking Trojan is Able to Infect PCs With Up-To-Date Anti-Virus .....	23
Site Offers Facebook Account Break-Ins for \$100 .....	23
Sophisticated Botnet Causing a Surge in Click Fraud .....	23
Botnet Discovered on Linux Servers .....	24
Joe Wilson's Payments Provider Reports DDoS Attack .....	24
<b>Cyberspace Tactics and Defense .....</b>	<b>25</b>
Raytheon Hires Air Force Network Operations Expert for Cybersecurity Post .....	25
Cisco Forms Smart Grid Ecosystem .....	25
Microsoft to Offer Free Antivirus Software .....	25
New Service Certifies Security of Printers, Copiers, Other Networked Devices .....	25
IETF Forges Botnet Clean-Up Standard .....	26
Google + reCAPTCHA Could Raise Bar in Anti-Bot, Anti-Spam Fight .....	26
Heartland CEO: Credit Card Encryption Needed .....	26
NRC, FERC to Cooperate on Cybersecurity for Nuke Plants .....	27
Cybercrime Fighters Adopt Community Tactics .....	27
Symantec Tool Calculates Your Data's Value to Thieves .....	27
<b>Cyberspace - Legal .....</b>	<b>28</b>
GOP Senators Move to Stop Obama Net Neutrality Rules .....	28
Republicans to Push Against Net Neutrality; FCC Says Start of Process .....	28
Presidential Internet Kill Switch May Still be Alive .....	28
Intelligence Analyst Says Hacking Charge Doesn't Compute .....	28
Cybersecurity Measure Takes A Back Seat for Co-Sponsors .....	29
Cerf: Turning Off Pieces of the Internet 'not sensible' as Security Strategy .....	29



# CyberPro

Volume 2, Edition 19  
September 24, 2009

## Keeping Cyberspace Professionals Informed

Trial Set for 'Botnet for Hire' Duo.....29

**Cyberspace-Related Conferences..... 30**

**Cyberspace-Related Training Courses ..... 32**

**Cyber Business Development Opportunities ..... 34**

**Employment Opportunities with NSCI..... 36**

**CyberPro Content/Distribution ..... 36**



### CyberPro™

Keeping Cyberspace Professionals Informed

**Subscribe  
Today!**

Go to:  
[www.nsci-va.org/CyberProNewsletter.htm](http://www.nsci-va.org/CyberProNewsletter.htm)

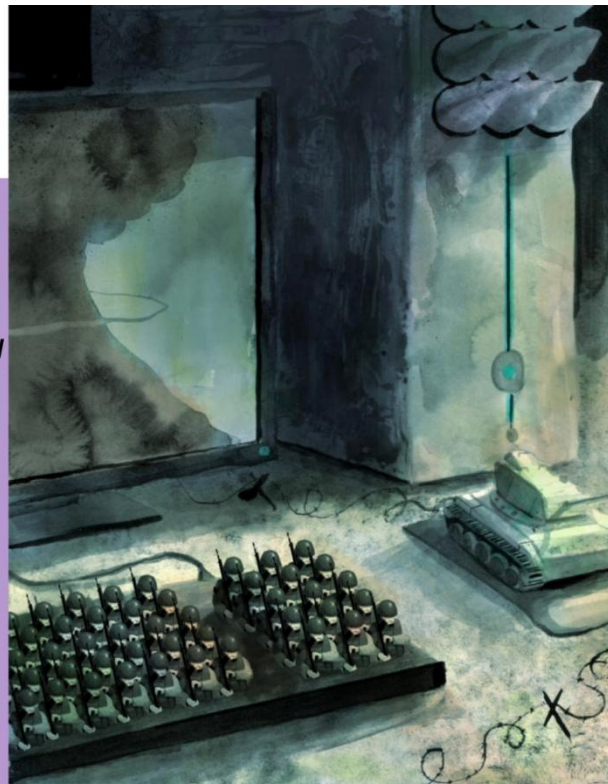


Illustration by [www.callicutart.com](http://www.callicutart.com) – NSCI Copyright 2009



## THIS WEEK IN CYBERPRO

BY LINDSAY TRIMBLE, NATIONAL SECURITY CYBERSPACE INSTITUTE, INC.

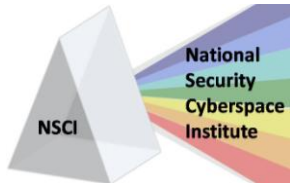
The Department of Homeland Security's (DHS) Philip Reitering, deputy undersecretary of the National Protection and Programs Directorate, said recently that hackers are becoming more organized in attacking critical government IT systems than government and businesses are at defending them ([page 18](#)). Reitering stressed to the Senate Committee on Homeland Security and Governmental Affairs that the government and industry must collaborate to develop better cyber defense solutions. Defense Tech's Kevin Coleman would agree. In an article this week, Coleman writes that while the Obama administration has said that cybersecurity is a major priority, there hasn't been the action to back up that statement ([page 12](#)).

The DHS is ready to take that action; an announcement was made recently that the organization will more than double the number of employees in their National Cybersecurity Division by next year ([page 17](#)). Dennis Blair, the director of national intelligence, is also prepared to increase cybersecurity efforts. U.S. intelligence agencies will enhance their cybersecurity mission over the next four years ([page 13](#)).

One area for increased concern among cybersecurity professionals is the lack of national cyber leadership. Representatives James Langevin (D-R.I.) and Michael McCaul (R-Texas) sent a letter to President Barack Obama this month, saying they were "deeply concerned by the delay" in appointing a federal cybersecurity coordinator ([page 16](#)). Defense Secretary Robert Gates recently suggested that the DHS and National Security Agency share the duties of cybersecurity head ([page 16](#)).

Along with leadership, another common theme is preparing the public to be on the cyber offensive. Internet users are increasingly being asked to prevent cyber attacks – by industry members and even the Federal Bureau of Investigation ([page 27](#)). Naval Postgraduate School Professor John Arquilla has said that the U.S. military should collaborate with network specialists around the globe to "launch preemptive online strikes" to stop real-world conflicts ([page 17](#)).

In the "Senior Leader Perspective" this week, I had the opportunity to chat with Rear Admiral Elizabeth Hight, vice director of the Defense Information Systems Agency ([page 6](#)). In our interview, Hight discusses key cyberspace-related programs that DISA has enacted to continue delivering cyber capabilities to the military. She also highlights the aspects of DISA that will change with the stand-up of the new U.S. Cyber Command, providing her insight as to how industry and academia will be able to contribute to the new organization.



### SENIOR LEADER PERSPECTIVE: RADM ELIZABETH HIGHT

NSCI's Lindsay Trimble recently interviewed Rear Admiral Elizabeth Hight, vice director of the Defense Information Systems Agency (DISA). In this role, Hight helps lead a worldwide organization of more than 6,600 military and civilian personnel responsible for planning, developing and providing interoperable, global net-centric solutions that serve the needs of the President, Secretary of Defense, Joint Chiefs of Staff, the combatant commanders and other Department of Defense components. Prior to this assignment, Hight was DISA's principle director for operations and deputy commander, Joint Task Force-Global Network Operations (JTF-GNO) from 2006 to 2007.



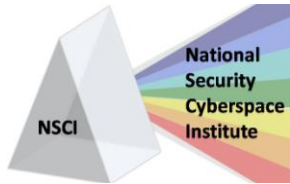
**NSCI: In 1991, DISA evolved from the Defense Communications Agency – an organization that consolidated the communications systems of the Army, Air Force and Navy. As cyber communications have come to the forefront, how has DISA continued to consolidate the work being done in each of the military services?**

REAR ADMIRAL ELIZABETH HIGHT: DISA doesn't really *consolidate* the work. Think of the world as a round globe and what DISA does is provide the "superhighway" around the world for all of the Services, agencies and Combatant Commands (COCOMs) to join up to. Think of what we provide as the "interstate system" and the Services, COCOMs and agencies have sort of "state roads" and "county roads" off of that great big "interstate" to get to their specific user base. So, we don't really consolidate; we provide the linking between either expeditionary users – meaning they don't have to be in one place all the time, such as a Navy ship – or a fixed base, in order to reduce costs.

**NSCI: How has the increase in cyberspace operations affected DISA's overall mission?**

HIGHT: We are finding ourselves reaching out into the combat zones to an even greater degree than we did in the past – out to what we call the "tactical edge." In the past, typically our support would be to a primary base of a Service or some other location and today, we reach our SATCOM systems and terrestrial links into the hills of Afghanistan, the outlying cities of Iraq, the major and rural areas of Korea and, you name it, we go way out to the edge to a much greater extent than we ever did in the past.

Now, what does that do for us? Let's take the Korean Peninsula as an example. If the Army, Navy, Air Force or Marine Corps on the Korean Peninsula had to buy or lease all of their own circuits on and off the peninsula, just imagine the cost of that. What we have done is taken their requirements for all peninsula communications – either terrestrial or satellite – and bundled them together in order to 1) provide a service, so they don't have to do that individually, and 2) to reduce cost.



## *Keeping Cyberspace Professionals Informed*

We then provide a link into that great big “interstate highway system” and then they can build whatever permanent or temporary “county roads” that they need to meet their requirements. So some requirements are standing requirements, especially the ones here in CONUS where you have a fixed based that has been there a long time and is likely to be there for a long time. So those requirements are well understood, but the expeditionary requirements – where we can take a big pipe into theater or other countries and then the Services pull not only their transport, but some capabilities off of that big pipe—allow them to respond very quickly and very dynamically to the world’s events.

***NSCI: With network centric operations, the ability to deliver information to our warfighters is more fluid and timely. But with the increasing use of computer networks, we become more dependent and reliant on systems that could – potentially – be victim to cyber attacks. Regarding cyberspace, how does DISA balance the potential risks with the immediate access warfighters have come to expect?***

HIGHT: We have embarked on redesigning the unclassified systems that the DoD uses – what we call the unclassified intranet for the department, referred to as the NIPRNET. Just like any very large organization, we have our own intranet and it has access to the Internet, but we protect that intranet very carefully. We are redesigning it with security in mind. We’re redesigning the NIPRNET and are looking at things that you would see out in the commercial world.

For example, if you were to go to Amazon.com to order a book, you would be able to see all of Amazon’s outward-facing information that they want you to see, such as their inventory list, their shipping options, the cost of their books, etc. You would not be able to see anything that they want to keep to themselves, like their financial data. We are redesigning the NIPRNET to include that kind of technology, so that only the information that we want to be seen by people in the Internet can be seen by them. We have several initiatives to protect information on the NIPRNET from people trying to access the information that’s not available to them.

***NSCI: From a DISA and Joint Task Force – Global Network Operations perspective, can you discuss a few of the key challenges regarding cyberspace operations?***

HIGHT: From both the DISA and the JTF perspective, the biggest challenge in cyberspace is “How do you share information while keeping a secret?”

You have a balance between what information is made available, through what means and to whom? In order to make those decisions, we think about risk. Of course, in the military, operational risk is a significant issue in anything that we do. In order to make a balancing decision between what we can share and what we keep a secret, we need to think hard about what the dynamics of a specific mission will require.

So let’s think for a moment about the continuum of missions that the department is expected to be ready to handle. We do everything from humanitarian assistance and disaster relief to sort of “showing the flag” and promoting U.S. interests through conflict all the way to government stabilization and



## *Keeping Cyberspace Professionals Informed*

keeping the peace. And so depending on which phase of that continuum we are in at any one time, our information sharing needs are different.

For instance, if we're in the middle of supporting Katrina or the tsunami relief effort or an earthquake relief effort, we often find ourselves working with organizations that we're unfamiliar with and with people that we don't know. Our information sharing has to be unrestricted by encryption and other techniques that we use to keep the secrets. On that end of the continuum, it's all about sharing information: Where do the next deliveries of water and food need to be? What is the potential landing zone for a helicopter delivering those goods? The dimension for information sharing on that part of the continuum is very high. The requirement to keep a secret is relatively low.

But, if you march through that continuum and you approach conflict, the requirements to share information with unanticipated users is typically reduced, because you know who you're dealing with in that conflict and your requirements to keep a secret are typically higher because you don't want the adversary to know what you're doing.

So throughout that entire continuum of operations, you make risk decisions based on the mission at the moment. So the network has to be flexible enough to work throughout that continuum. Our ability to share information while keeping a secret – which is different for each situation – has to be enabled by the network.

***NSCI: Can you tell us about a few of the key cyberspace-related programs (e.g. HBSS-Host-Based Security System) that DISA and/or JTF-GNO are using to deliver capabilities to Combatant Commands and/or Services?***

HIGHT: Yes, we have a plethora of them. We have everything from tools that allow us to understand the readiness of our networks; tools that allow us to understand anything that's going wrong in the network; tools that allow us to configure our networks automatically or to know when a network goes out of configuration. We also have tools that allow us to understand what is coming into the NIPRNET from the Internet; tools that allow us to understand what's coming from the NIPRNET to the Internet, so we know what's going out into the public domain. We have tools that will allow us to segregate the outward-facing databases – we can segregate those from information that shouldn't be accessed from the Internet. We have a lot of tools.

One of the things that is important to know is that the JTF – soon to be part of the U.S. Cyber Command – is an operational command that determines what requirements need to be met and DISA is a technology and engineering organization that develops and provides those tools. That symbiotic relationship of what the users need and how DISA can get them into the field has been one of the hallmarks of what we've accomplished in the last several years. That will not change when the JTF moves to Fort Meade and becomes part of the Cyber Command because it will always be the responsibility of the operational command to define the requirements and it will always be the responsibility of the engineering and technical organizations to try to meet those requirements.

---

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



## *Keeping Cyberspace Professionals Informed*

***NSCI: How do you see the increased demands of standing up the new U.S. Cyber Command affecting DISA and JTF-GNO's ability to continue fulfilling responsibilities that were already herculean?***

HIGHT: Certainly, the requirements are not going to be reduced in any way. I think the task before us – as U.S. Cyber Command stands up is to ensure that we retain our strong relationship with that operational command. We don't let the mission fail right now. DISA and the JTF-GNO work the net ops hand-in-hand and our No. 1 priority is to ensure that the net ops mission continues to exert a strong command-and-control logic on the networks and that there is a single organization in charge of directing the operation and defense of the networks.

In terms of day-to-day activities, there won't be a whole lot that will change. In terms of organizational structure, of course there will. Today, the JTF-GNO and DISA are co-located in the same operations center. They sit side by side and as things happen on the network, there are technical experts from the DISA team that will help the JTF team and JTF operators will identify ongoing operational requirements that DISA needs to respond to. As we look end-to-end at any one moment in time, between the point where one person is talking to another, there might be many different networks involved. So if I'm sitting on a Navy ship and I want to communicate with my Air Force brethren in an operation, I will send out information from my ship on a Navy network that goes to a network operations center. The Navy Network Operations Center is connected to the big "interstate highway" we call the Global Information Grid. That information now has flowed over the Navy network, over the big enterprise network that DISA manages, onto an Air Force network that will eventually make its way to the Air Force expeditionary unit also in the operation.

When we talk about the network, we're not looking at a homogenous system. We're looking at a network of networks. So the DISA team that sits in the same ops center as the JTF-GNO can immediately respond to the JTF with what's going on in the big "interstate highway." So, what we have to do is go to the Services and get out the "county cops" and let them tell you what's going on on those "county roads." The ability to have an end-to-end view of information flowing from source to destination is still a work in progress. We have a very strong command-and-control relationship between the JTF and the owners of the networks – one of which is DISA – to make sure we can understand that end-to-end capability.

As in most things related to technology, we are still learning and we still have a ways to go to get extremely accurate end-to-end situational awareness. I think the more that we use the networks and the more netcentric we become, the more we will begin to require machine-to-machine capability that can be reported automatically and not manually.

***NSCI: With the stand-up of USCYBERCOM, there will obviously be some changes in the command and control of cyberspace. Are there any areas where industry and/or academia could contribute?***



HIGHT: Absolutely! If you think about America 100 years ago, we had an awful lot of cow paths and horse trails and not very many roads. Think about America today; that's the same analogy you can apply to the network.

As the networks grow and proliferate, we need a strong industry commitment to both develop systems that can be adopted in a netcentric view; we need data that can be published and subscribed to within the netcentric framework; we need to advance the capabilities of understanding how to prioritize information based on mission requirements in something similar to a quality-of-service prioritization key. We need to continue to adopt a unified communications approach, where we don't reserve this particular part of the network for voice, this particular part of the network for video and this particular part of the network for data, but we need to let all three mediums travel on the network and let the operational commanders decide what they want to allocate to which technology. There are a huge number of issues associated with the netcentric world of tomorrow.

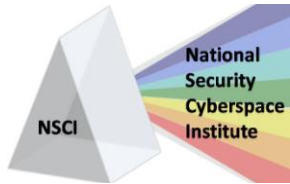
There's another area in which industry and academia could contribute. Right now today, we manage IT networks terrestrially differently from how we manage IT networks over satellite communication. We can't do that in the future. We need to be able to have that situational awareness and that command of the network to allow for a flexible and dynamic response based on the mission that's underway at the time.

The military today is incredibly dependent on information – real-time information delivered at the right time in the right format. We simply cannot have a military that has to take all of that information with them all of the time. What we need, instead, is a way for that soldier, sailor, airmen or marine or coast guardsman to be able to reach into a data store that is authoritative and up-to-date – immediately, wherever they are on the face of the planet and get the information that they need.

So industry and academia can help us by furthering the concepts of what many people refer to as cloud computing, and what I would refer to as netcentric involvement – where the data resides is irrelevant to whether or not you can get it to the user who needs it. We continue to look at concepts where data is available on demand; bandwidth is available on demand; it can be managed dynamically and in real-time; and it is not hampered by distance or geography. It will take a partnership to make it happen.

***NSCI: There has been a lot of press recently regarding DoD policy on the use of social networking and Web 2.0 tools. Can you clarify what the current policy is, and tell us about some of the risks and benefits – from DISA and JTF-GNO perspective – being considered?***

HIGHT: As you know, the current policy is under review by the community – that being all of us who are stakeholders in both the use of the network and the use of the information that travels over the network. The current policy does not restrict the use of social networking sites. There are concerns – not only about malicious activity that might be occurring on a social networking site, but on anything that might be brought back into the NIPRNET as malicious software. There are concerns about the incredible



increase in the bandwidth required to access these sites from government computers that are meant for mission purposes and there are concerns over operational security.

Just as I described the risk equation for operational missions, we are looking hard at what the risk equation is for the use of computers from our NIPRNET into the Internet and whether or not our policies meet the need to share information while keeping a secret. I would say that there are some members of the Department of Defense that absolutely rely on social networking sites and we do not want to reduce their ability to use them, but what we might end up doing is having a combination of policies, procedures and technology that would allow us to share information while keeping a secret. That, of course, is the goal.

***NSCI: Is there anything else you'd like to add?***

HIGHT: This is the most exciting time in cyber technology that I have ever witnessed. I've been doing this for a few years. There are a lot of things that we still have to accomplish. We're on a long road; we're on a journey to understanding how we can utilize capability in order to advance the nation's goals and protect our people.

The entire DISA team would welcome good ideas, we would welcome leveraging, we would welcome collaboration – all within the bounds of what federal law allows us to do. I think we have a long journey to go together and I think this stuff is way cool and a lot of fun.



### CYBERSPACE – BIG PICTURE

#### **The Five Most Dangerous Internet Security Myths**

BY: MIRIAM BOBROFF, EZINE ARTICLES  
09/22/2009

This article discusses five Internet security “myths” and why they may not be helping Internet users stay safe online. The article says that hackers are no longer teenagers looking for fame, but are now organized crime groups that are financially motivated. The article also says that users need to have antispyware, antirootkit and a bidirectional firewall installed on their machines in addition to an antivirus program. Hackers are increasingly using personal pages and big-name company sites to spread malware, so simply being careful of where you surf is no longer adequate protection.

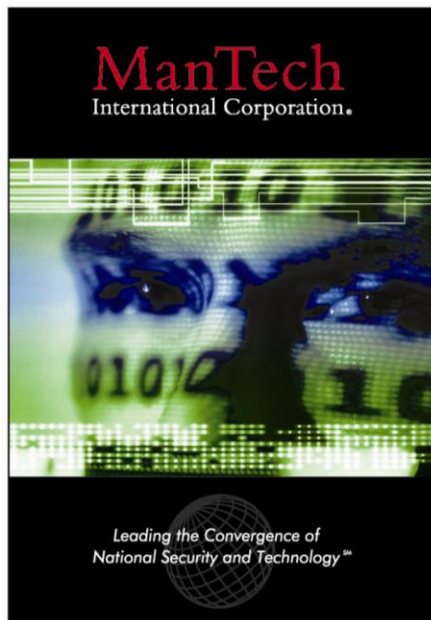
<http://ezinearticles.com/?The-Five-Most-Dangerous-Internet-Security-Myths&id=2884355>

#### **There’s Concern, But Where’s the Action?**

BY: KEVIN COLEMAN, DEFENSE TECH  
09/21/2009

The problem of cybersecurity has been called “as significant as that of Iran having developed a nuclear weapon” and the Pentagon’s Strategic Command tells Congress that the United States is “vulnerable to cyber attacks across the spectrum.” President Barack Obama has said that “the nation’s digital infrastructure is under near constant attack.” Suleyman Anil of NATO says that cybersecurity is considered to be at the same level as missile defense and energy security. In this article, Kevin Coleman asks why there is not more being done to improve cybersecurity, when so many recognize the severity of cyber threats.

<http://www.defensetech.org/archives/005025.html>



#### ***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 – U.S. GOVERNMENT

### **FCC Chair Proposes ‘Open Internet’ Rules**

BY: PETER SVENSSON, WASHINGTON TIMES  
09/21/2009

Federal Communications Commission chairman Julius Genachowski says that wireless carriers should be subject to “open Internet rules” and should not be able to block certain types of Internet traffic from flowing over their networks. Genachowski says that the same rules the FCC already applies to wired Internet traffic should be extended to wireless. The FCC wants a formal rule saying that Internet carriers cannot discriminate against any type of traffic by degrading service. Consumer advocates and some Web companies want to “safeguard what has been an underlying ‘Net Neutrality’ assumption of the Internet: that all traffic is treated equally by the network.”

<http://www.washingtontimes.com/news/2009/sep/21/fcc-chairman-proposes-open-internet-rules/>

### **FCC Chairman Expected to Outline Net Neutrality Rules**

BY: MIKE KENT, NEWSFACTOR.COM  
09/18/2009

Julius Genachowski, the Federal Communications Commission Chairman, is expected to outline network-neutrality proposals that would keep Internet service providers from blocking or slowing Internet traffic based on content. ISPs such as Verizon and AT&T say that growing traffic needs to be better managed and that neutrality would stifle Internet innovation. Ben Scott, policy director of Free Press, says that they are pleased that the FCC is “protecting the open Internet’s free market for speech and commerce.”

[http://www.newsfactor.com/story.xhtml?story\\_id=69052](http://www.newsfactor.com/story.xhtml?story_id=69052)

### **Feds Can Monitor Personal E-Mail Sent Privately to Gov’t Workers, DOJ Says**

BY: MARTHA NEIL, ABA JOURNAL  
09/21/2009

A recently published legal opinion from the U.S. Department of Justice says that both recipients and senders of e-mails that go to government employees logged into a work computer network are subject to monitoring by the federal government. David Barron, acting assistant attorney general, says that federal employees automatically give their permission for the government to monitor their communications; when they log on to government computes, they receive a notice from the Homeland Security Department that says that their machines are being monitored for malicious intrusions. Someone sending e-mail to a federal employee must also assume that the e-mail could be read.

[http://www.abajournal.com/news/feds\\_can\\_monitor\\_private\\_email\\_sent\\_to\\_govt\\_workers\\_doj\\_says/](http://www.abajournal.com/news/feds_can_monitor_private_email_sent_to_govt_workers_doj_says/)

### **Intell Agencies Plan to Beef Up Cybersecurity**

BY: BEN BAIN, FEDERAL COMPUTER WEEK  
09/15/2009

The 2009 National Intelligence Strategy from the Office of the Director of National Intelligence says that enhancing cybersecurity is a mission objective for intelligence agencies during the next four years. Dennis Blair, the director of national intelligence, says that the United States must be more aggressive in cyber operations and identified China and Russia as the most aggressive nations in the cyber world. The NIS report says that the architecture of the nation’s digital infrastructure is not secure or resilient, and that intelligence agencies need to integrate cyber expertise throughout agencies



and pay more attention to neutralizing cyber threats.

<http://fcw.com/articles/2009/09/15/web-nis-cybersecurity.aspx>

### **Committee Examines Growing Cyber Threat to Businesses**

TMCNET  
09/15/2009

Homeland Security and Governmental Affairs Chairman Joe Lieberman (I-Conn.) and Ranking Member Susan Collins (R-Maine) have explored the threat of cybercrime to small- and mid-sized businesses and discuss how the federal government can help businesses defend themselves. Lieberman and Collins are drafting legislation that will address cyber security issues. Lieberman says that a public-private partnership to defend cyberspace is essential and that businesses, government and law enforcement agencies worldwide must work together to combat cyber threats. Collins says that the new legislation will address attacks against individuals, businesses and government and also says that the government needs to make cybersecurity a higher priority, and work to form a public-private partnership.

<http://www.tmcnet.com/usubmit/2009/09/15/4372163.htm>

### **Government Should Help Widen Cyber Knowledge**

BY: MAX STIER, FEDERAL TIMES  
09/14/2009

The Partnership for Public Service recently released a study that found that federal officials and other experts agree that the government must address its "shortage of technically sophisticated professionals capable of combating the growing cyber threat from hackers, criminals, foreign governments and terrorist organizations." The report said that there has been a lack of high-level federal leadership, and also discussed the lack of training for workers and a clear career path or certification system for cybersecurity specialists. Max Stier writes that the government must assess its workforce needs, develop a plan for recruiting workers and then focus on hiring and retaining cybersecurity talent. Stier also says that the government should look into encouraging universities to offer cybersecurity programs.

<http://www.federaaltimes.com/index.php?S=4273437>

You need to focus on dozens of tasks each second in order to keep information operations at full speed. Being concerned about the security of your information shouldn't be one of them. Whether your mission is to secure information from a crime scene or prevent network intrusions, ITT makes it our mission to relieve that concern. We provide the most comprehensive suite of tools available to ensure that your information arrives at its destination, without compromising data integrity and timeliness. Learn more at [aes.itt.com](http://aes.itt.com).

## In the world of information security, second place is not an option.



Communications • Sensing & Surveillance • Space • Advanced Engineering & Integrated Services

ITT, the Engineered Blocks logo, and ENGINEERED FOR LIFE are registered trademarks of ITT Manufacturing Enterprises, Inc., and are used under license. © 2009, ITT Corporation.



### Cyber Criminals Targeting Small Businesses

BY: LOLITA C. BALDOR, YAHOO TECH  
09/14/2009

Federal authorities warn that cyber criminals are increasingly targeting small- and mid-size businesses that do not keep their computer security tools updated. Michael Merritt, assistant director of the U.S. Secret Service's office of investigation, explains that larger companies have taken on more sophisticated computer network protections, leaving small- and mid-size businesses more vulnerable to attacks. Phil Reitingger, the deputy undersecretary of the Department of Homeland Security, says that businesses can use better antivirus and antispyware programs to protect themselves. Reitingger also says that government agencies must improve coordination with each other and the private sector to better protect businesses.

[http://tech.yahoo.com/news/ap/20090914/ap\\_on\\_hi\\_te/us\\_cyber\\_crime\\_small\\_business](http://tech.yahoo.com/news/ap/20090914/ap_on_hi_te/us_cyber_crime_small_business)

### Republican Lawmakers Want Answers from ICANN

BY: ANDREW NOYES, CONGRESSDAILY  
09/16/2009

In a letter to Rod Beckstrom, CEO of the Internet Corporation for Assigned Names and Numbers, House Judiciary Committee's ranking member Lamar Smith and Courts and Competition Subcommittee ranking member Howard Coble said they are concerned over the introduction of new top-level domains such as .info and .us. The U.S. Chamber of Commerce and National Association of Manufacturers say that the expansion of domains could cause an increase in "cyber-squatting, fraud and overall confusion in the Internet marketplace." Smith and Coble have asked for details from ICANN about the termination of the joint project between ICANN and the U.S. government which is scheduled for later this month.

[http://www.nextgov.com/nextgov/ng\\_20090916\\_9990.php](http://www.nextgov.com/nextgov/ng_20090916_9990.php)

**Assess, Detect, Respond, Secure**  
with a Cybersecurity Solution Built on Forensically Sound Technology

**EnCase Cybersecurity**

- Proactively identify and recover from covert network threats and classified spillage
- Detect polymorphic malware over the network
- Ensure endpoints remain in a trusted state

Delivering cybersecurity and forensic solutions to government agencies for more than 10 years.  
Learn More >>> visit [www.guidancesoftware.com](http://www.guidancesoftware.com) or call 1-866-973-6577

**Guidance SOFTWARE**  
The World Leader in Digital Investigations



## U.S. CYBER LEADERSHIP DEBATE

### Pressure Builds on Obama to Appoint Cybersecurity Coordinator

BY: BEN BAIN, FEDERAL COMPUTER WEEK  
09/14/2009

Reps. James Langevin (D-R.I.) and Michael McCaul (R-Texas) recently sent a letter to President Barack Obama saying they were pleased with the progress on creating a comprehensive national security strategy for cyberspace, but that they were “deeply concerned by the delay” in appointing a federal cybersecurity coordinator. Obama announced in May that he would set up a new White House cybersecurity office led by a coordinator that he would appoint, and the Congressmen now urge him to “solidify” his early cybersecurity efforts by “swiftly appointing a cybersecurity coordinator.”

<http://fcw.com/articles/2009/09/14/web-cyber-coordinator-urged.aspx>

### Gates: No New Cyber-Eavesdropping Agency

BY: BEN IANNOTTA, C4ISR JOURNAL  
09/17/2009

Defense Secretary Robert Gates says that the United States does not have enough money or people to create a separate National Security Agency to be responsible for cyberspace. Gates suggests that the Obama administration assign an official a “double-hat” role as cybersecurity head at both the Department of Homeland Security and the National Security Agency. Gates says that he has also directed the military services to make cybersecurity training a top priority.

<http://www.c4isrjournal.com/story.php?F=4282052>

## CYBERSPACE – DEPARTMENT OF DEFENSE (DoD)

### Balancing Social Networking and Cybersecurity

BY: MICHAEL HOFFMAN, AIR FORCE TIMES  
09/21/2009

This article includes an interview with Gen. Robert Kehler, head of the Air Force’s Space Command. Kehler says that the Air Force has not yet decided what it will do regarding social networks such as Facebook and Twitter, but that completely blocking the sites would be “extreme.” Kehler also says that there has been more focus on cyber security capabilities since the stand-up of the 24th Air Force, which will work to understand the Air Force network and improve the capabilities to better support U.S. Cyber Command. Kehler added that airmen that work under the cyberspace mission will operate

and defend the network, and will also conduct offensive operations if directed. Finally, Kehler says that the Air Force has been putting IT acquisition programs in place for years, and is working with Material Command to ensure the security of software used on Air Force networks.

[http://www.airforcetimes.com/news/2009/09/airforce\\_afa\\_space\\_092109w/](http://www.airforcetimes.com/news/2009/09/airforce_afa_space_092109w/)

### Cyber Threat Calls for Flexibility in Command Model, General Says

BY: AMBER CORRIN, FEDERAL COMPUTER WEEK  
09/18/2009

Lt. Gen. William Lord, chief of Warfighting Integration and chief information officer of the Office of the Secretary of the Air Force, says



## Keeping Cyberspace Professionals Informed

that cyberspace has changed the way military commands should be structured, and that the Air Force is already heavily engaged in cyber operations. Lord explained that U.S. Cyber Command and other military forces need to create a flexible command structure that incorporates non-traditional elements. He added that superiority in cyberspace is “required for operational freedom of action” and that there is a “need for the discipline and vigor of the traditional command model.”  
<http://fcw.com/articles/2009/09/18/lord-emphasizes-joint-force-approach-to-battle.aspx>

### **John Arquilla: Go on the Cyberoffensive**

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK  
09/21/2009

Naval Postgraduate School Professor John Arquilla says that the U.S. military should team up with network specialists around the world to

“form a global geek squad” that would “launch preemptive online strikes” to stop real-world conflicts. For example, Pakistan and India are currently gathering forces on their shared border. Arquilla recommends that this global “geek squad” use an online strike to take out the command-and-control networks on both sides so that the nuclear-armed countries do not go to war. Arquilla also recommends using this strategy against al-Qaeda and other terrorist groups that are increasingly dependent on the Internet for communication. Arquilla says that this approach would be a “nonlethal way to deter lethal conflict” and also a “kinder, gentler deterrence” than threatening to attack an adversary.  
[http://www.wired.com/techbiz/people/magazine/17-10/ff\\_smartlist\\_arquilla](http://www.wired.com/techbiz/people/magazine/17-10/ff_smartlist_arquilla)

## CYBERSPACE – DEPARTMENT OF HOMELAND SECURITY (DHS)

### **Authentication Said Key to Cybersecurity**

BY: BEN BAIN, FEDERAL COMPUTER WEEK  
09/22/2009

Bruce McConnell, cybersecurity counselor to Philip Reitinger, the Homeland Security Department’s principal cybersecurity official, says that authentication is a major part of DHS’ vision for improved cybersecurity. McConnell says that DHS wants an open, standards-based cyber system that is securely designed and that would be supported by metrics that can help with budgeting cybersecurity funds. McConnell says that better authentication would reduce the complexity of intrusion detection and that a digital authentication system needs to be voluntary, easy to use, able to support multiple roles in cyberspace and would adhere to the worldwide list of fair information practices that relate to privacy and also provide anonymity.

<http://fcw.com/articles/2009/09/22/web-mcconnell-cybersecurity.aspx>

### **Homeland Security to More Than Double Staff for Cyber Threats**

BY: JEFF BLISS, BLOOMBERG  
09/14/2009

The Department of Homeland Security recently announced they will more than double the number of employees in one of their cybersecurity units by next year. Philip Reitinger, deputy undersecretary of the National Protection and Programs Directorate at DHS, says that more employees are needed as cyber threats become increasingly dangerous and because attacks continue to become more sophisticated and complex. DHS will increase the National Cybersecurity Division workforce, which analyzes and responds to computer



## Keeping Cyberspace Professionals Informed

attacks on the government and companies that provide services such as electricity and phone transmission.

<http://www.bloomberg.com/apps/news?pid=20601087&sid=ayDCHq5H0CH8>

### **Testimony: Hackers Better Organized than Government**

BY: ERIC CHABROW, GOVERNMENT INFORMATION SECURITY

09/14/2009

Philip Reiting, DHS deputy undersecretary of the National Protection and Programs Directorate, recently told the Senate Committee on Homeland Security and Governmental Affairs that hackers are

becoming better at information sharing and more organized in attacking critical government and business IT systems than the government and business are at defending their cyber assets. DHS Assistant Director Michael Merritt of the Secret Service's Office of Investigations says that carding portals allow criminals to link up anonymously and share hacking tools and information. Reiting says government and business must partner up to develop better cyber defense solutions, including new ways of authenticating users without requiring usernames and passwords.

[http://www.govinfosecurity.com/articles.php?art\\_id=1775](http://www.govinfosecurity.com/articles.php?art_id=1775)

**Emerging technologies.**

**Unpredictable threats.**

**Elusive enemies.**

**Ready for what's next.** Now more than ever, mission success depends on the ability to continually adapt thinking and operations. With the perspective, experience, and know-how from battlefields and boardrooms, the strategy and technology consultants of Booz Allen Hamilton can help you achieve your cyber goals. Whether you're managing today's issues or looking beyond the horizon, count on us to help you be ready for what's next.

**Booz | Allen | Hamilton**  
delivering results that endure

Ready for what's next. [www.boozallen.com](http://www.boozallen.com)



## CYBERSPACE – INTERNATIONAL

### How is Government Coping with Cyber Crime?

BY: ROBIN HICKS, FUTUREGOV  
09/22/2009

Author Robin Hicks spoke with senior civil servants in Taiwan, Hong Kong, China and the Philippines to see how each country is preparing their defenses against hackers and cyber criminals. Hsiang-Chen Li, director of the Computer Centre for the National Police Agency in Taiwan, says that Taiwan has a Computer Crime Squad within their police department, and has also established N-CERT and N-SOC – initiatives to protect information infrastructure. Pang Yandong, director of the Information Industry Office for the Government of Maoming City in China, says that China is working to strengthen its information security system and to increase user awareness of information security through training and keeping the most up-to-date security settings on all computers. Stephen Mak, deputy government chief information officer for Hong Kong, says that Hong Kong has established the Computer Emergency Response Team Coordination Center (HKCERT) to monitor cyber threats, and government departments have also implemented technical security measures and established incident response and business continuity plans. Finally, Ray Roxas-Chua, chairman for the commission on Information and Communications Technology in the Philippines, says that the commission is working to push the passage of an anti-cybercrime bill similar to the Convention on Cybercrime by the Council of Europe. The commission is also in the process of setting up a national public key infrastructure to ensure safer online transactions.

<http://www.futuregov.net/articles/2009/sep/2/how-government-coping-cyber-crime/>

### MI5 Ropes in Teenage Hackers to Combat Cyber Terrorism

INFOWAR  
09/22/2009

The British Intelligence Agency MI5 has hired approximately 50 new computer-savvy hackers, including many teenagers, to work in the new Cyber Operations Command. The new employees have signed the Official Secrets Act which prevents them from telling their families and friends about the work they are doing. A report in the British Sunday Express also said that the new workers, including the teenagers, are subject to the same level of background security checks as other intelligence staff. The new Cyber Operations Command has been directed by MI5 head Jonathan Evans to combat cyber warfare, especially threats from China, Russia and Pakistan.

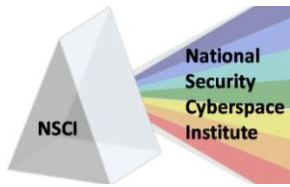
<http://www.infowar.com/2009/09/22/mi5-ropes-in-teenage-hackers-to-combat-cyber-terrorism/>

### South Korea to Train 2,000 'Cyber Sheriffs:' Report

SPACEWAR  
09/13/2009

According to the Yonhap news agency, South Korea is planning to train 3,000 cyber sheriffs who will work to protect corporate information and prevent industrial data leaks. South Korea already has a military cyber unit and, in the case of a cyber attack, the South Korean National Intelligence Service would create a taskforce of civilian and government experts to counter online threats. South Korea and the United States were recently the victims of online attacks which targeted U.S. and South Korean government Web sites.

[http://www.spacewar.com/reports/SKorea\\_to\\_train\\_3000\\_cyber\\_sheriffs\\_report\\_999.html](http://www.spacewar.com/reports/SKorea_to_train_3000_cyber_sheriffs_report_999.html)



### The South Asian Cyber War Threat

STRATEGY PAGE

09/17/2009

This article discusses how India and Pakistan are improving their cyber war capabilities. India has reportedly been turning to Israel for help in protecting itself against cyber war threats, while Pakistan is looking to China for cyber warfare technology. Two years ago, Pakistan established its Center for Cyber Crime because of Islamic terrorists that had been using the Internet for

communication and also because of Pakistan's dependence on Internet access. The ongoing "war" between Indian and Pakistani hackers has also made each of the governments look for better technology. India, in particular, "has one of the largest Internet software and service industries on the planet," and would be a prime target for Pakistani hackers.

<http://www.strategypage.com/htmw/htiw/articles/20090917.aspx>

**NORTHROP GRUMMAN**

*In today's world of cybersecurity, you'll need more than a firewall to keep from getting burned.*

[www.northropgrumman.com/cybersecurity](http://www.northropgrumman.com/cybersecurity)

▼ To really beat the bad guys, you need people not just computer programs. And Northrop Grumman has the expertise and the tools to keep your worst fears from coming true. This is the world of cybersecurity. A world we call home and know better than any other company in the industry. So when you're ready to talk to the experts about cybersecurity, come talk to us at Northrop Grumman.

**THE FACE OF CYBERSECURITY.**

©2009 Northrop Grumman Corporation

## CYBERSPACE RESEARCH

### Researchers Overwhelming Vendors with Security Flaws

BY: JOHN E. DUNN, TECHWORLD

09/16/2009

The Top Cyber Security Risks report from SANS has found that security researchers are uncovering so many flaws that it is difficult for vendors to patch them all in a reasonable timeframe. Attackers are increasingly using

application vulnerabilities to compromise systems, while server-side and OS flaws are declining. The report also says that there is a shortage of highly-skilled vulnerability researchers working for government and software vendors which creates a "significant disadvantage in protecting their systems against zero-day attacks." Software vendors need to employ more researchers to stay on top of

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



discovering and patching vulnerable applications.

<http://news.techworld.com/security/3201966/researchers-overwhelming-vendors-with-security-flaws/>

### **Microsoft Internet Explorer SSL Security Hole Lingers**

BY: TIM GREENE, NETWORK WORLD  
09/18/2009

Microsoft says that it is “still evaluating” whether a weakness in its Internet Explorer browser exists. The weakness was first pointed out seven weeks ago, and allows hackers to hijack secure Web sessions. A Microsoft spokesperson says that they are looking into the “possible vulnerability” but Apple has reported that the vulnerability exists in its Safari for Windows browser, which was based on Microsoft code. When exploited, the weakness allows man-in-the-middle attackers to trick the browser into making SSL sessions with malicious servers rather than the actual servers that users intend to connect to.

<http://news.techworld.com/security/3202232/microsoft-internet-explorer-ssl-security-hole-lingers/>

### **Snow Leopard Less Secure than Windows, Says Hacker**

BY: GREGG KEIZER, COMPUTERWORLD  
09/15/2009

Charlie Miller, Independent Security Evaluators, says that Snow Leopard lacks security features that come built-in to Windows XP, Windows Vista and Windows 7. Address Space Layout Randomization (ASLR) randomly assigns data to memory which makes it more difficult for hackers to find the location of critical operating system function. Miller says that Apple has not improved ASLR from Leopard to Snow Leopard, and explained that Apple’s ASLR does not randomize important components of the operating system. Miller also says that Apple

did improve security of QuickTime and added data execution prevention, a security feature used in Windows Vista. Miller believes that Macs are easier to compromise than Windows Vista systems because Snow Leopard lacks fully-functional ASLR, although Macs may still be safer because of hacker disinterest due to Apple’s smaller market share.

<http://news.techworld.com/security/3201863/snow-leopard-less-secure-than-windows-says-hacker/>

### **Botnet PCs Stay Infected for Years**

BY: JOHN E. DUNN, TECHWORLD  
09/16/2009

Analysis from security vendor Trend Micro reveals that PCs controlled by botnets may stay infected for years. Trend Micro looked at 100 million compromised IP addresses and found that 80 percent stayed compromised for more than a month, while the global median time for infection was more than 300 days. Trend Micro also found that the three largest botnets were Koobface, the Zeus or Zbot botnet, and Ilomo/Clampi. According to Trend researchers, more than 90 percent of all e-mail worldwide is spam.

<http://news.techworld.com/security/3201932/botnet-pcs-stay-infected-for-years/>

### **The Internet is the new Wild West, reports IBM Consultant**

BY: SUBATRA SUPPIAH, TECHWORLD  
09/11/2009

The 2009 Mid-Year Trend and Risk Report from X-Force found a 508 percent increase in new malicious Web links discovered in the first half of this year. There was a large increase in malicious content on trusted sites including online magazines, mainstream news sites and search engines. In response to the report, Sukhdev Singh, senior security consultant and regional X-Force expert, says that “safe browsing does not exist” and that we are at “a



## Keeping Cyberspace Professionals Informed

point where every Web site should be viewed as suspicious and every user at risk." The report also found that PDF vulnerabilities have increased, phishing attacks have decreased dramatically and that image-based spam is making a comeback. Sukhdev blames the applicant developers rather than the operating system or Web server vendors for the increase in malware, saying that Web application developers need to have pre-release code checks that would help to prevent some attacks.

<http://news.techworld.com/security/3201556/the-internet-is-the-new-wild-west-reports-ibm-consultant/>

### **Phishing Attacks Fell by 45% in August**

BY: CARRIE-ANN SKINNER, PCADVISOR  
09/10/2009

Symantec's State of Phishing report for September found that phishing attacks decreased by 45 percent in August, and that financial and online shopping sites were still most targeted by phishing scams. The report warns that phishing scams urging recipients to change their e-mail client application using a link in the e-mail have surged. Symantec says that the drop in phishing scams is most likely short-term.

<http://www.pcadvisor.co.uk/news/index.cfm?RSS&NewsID=3201469>



### **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 HACKS AND ATTACKS

### **New York Times Scareware Attack Shows Weakness of Ad Networks**

BY: DENNIS FISHER, THREATPOST  
09/15/2009

Online attackers were recently able to purchase ads that appear on the main page of the New York Times Web site, and are using the ads in scareware schemes that trick users into visiting malicious sites that install malware on the users' PCs. In this particular scheme, the attackers displayed legitimate ads for a few days and then replaced them with the

scareware ads, which told users that their PCs were infected and tricked them into buying fake antivirus applications. Several other media sites, including Fox News and the San Francisco Chronicle, were targeted in similar scans.

<http://www.threatpost.com/blogs/new-york-times-scareware-attack-shows-weakness-ad-networks-115>



### **Steganography Meets VoIP in Hacker World**

BY: TIM GREENE, NETWORK WORLD  
09/11/2009

Chet Hosmer, co-founder and Chief Scientist at WetStone Technologies, says that hackers are beginning to develop ways of stealing proprietary information from networks by hiding the information in VoIP traffic. This technique, called VoIP steganography, allows hackers to hide information within VoIP streams without even degrading the quality of calls. This article discusses the different techniques that hackers could use to hide information in VoIP traffic, such as using unused bits within UDP or RTP protocols for carrying the information or hiding data inside each voice payload packet. Hosmer reports that interest in steganography is increasing among criminals, and says that he is hoping to receive a Small Business Innovation and research (SBIR) grant from the government to begin work on developing his steganography jamming technology into a commercial product. <http://www.networkworld.com/news/2009/09/1109-steganography-meets-voip.html>

### **Zeus Internet Banking Trojan is Able to Infect PCs With Up-To-Date Anti-Virus**

SECURITY PARK  
09/21/2009

The Zeus online banking Trojan is considered the "most prevalent financial malware on the Internet today" and waits for users to log-on to targeted bank and financial institution Web sites, stealing their banking credentials or passwords. The Trojan affects machines that are running up-to-date antivirus programs almost 77 percent of the time. According to a report from Trusteer, 31 percent of machines infected with the Zeus Trojan had an antivirus product installed, 14 percent had outdated antivirus software and 55 percent had up-to-date antivirus protection installed.

[http://www.securitypark.co.uk/security\\_article/263686.html](http://www.securitypark.co.uk/security_article/263686.html)

### **Site Offers Facebook Account Break-Ins for \$100**

BY: JAIKUMAR VIJAYAN, COMPUTERWORLD  
09/18/2009

Security vendor PandaLabs reports that they have found an online service that will hack into any Facebook account for \$100. Users of the service are required to register with the Facebook hacking site, and then provide an ID of the Facebook they want hacked. When the hacking service has the password for the targeted Facebook account, the user must send \$100 via Western Union before they are given the password. Luis Corrons, technical director of PandaLabs, believes the site is meant to trick users into sending money, and may not actually provide any login information for the Facebook accounts. Corrons also says that victims of the scam are unlikely to report to law enforcement. [http://www.computerworld.com/s/article/9138258/Site\\_offers\\_Facebook\\_account\\_break\\_ins\\_for\\_100](http://www.computerworld.com/s/article/9138258/Site_offers_Facebook_account_break_ins_for_100)

### **Sophisticated Botnet Causing a Surge in Click Fraud**

BY: JUAN CARLOS PEREZ, COMPUTERWORLD  
09/17/2009

According to Click Forensics, a company which monitors ad campaigns for click fraud, botnets are now able to mask themselves as legitimate traffic so well that they are "skirting the most sophisticated filters of search engines." Click fraud affects marketers who spend money on pay-per-click (PPC) advertising, in which a person or machine clicks on a PPC ad with malicious intent. For example, a competitor might click on a rival's ad to drive up their ad spending, or a Web publisher might click on PPC ads on their site to trigger more commissions. Click Forensics reports that click fraud



scammers are increasingly using botnets in click fraud schemes.

[http://www.computerworld.com/s/article/9138213/Sophisticated\\_botnet\\_causing\\_a\\_surge\\_in\\_click\\_fraud](http://www.computerworld.com/s/article/9138213/Sophisticated_botnet_causing_a_surge_in_click_fraud)

### **Botnet Discovered on Linux Servers**

THE H SECURITY

09/14/2009

Analysis by Web developer Denis Sinegubko found that a network of hijacked Linux servers is being used to spread malicious software to Windows PCs. Sinegubko says that the compromised systems appear to operate normally, although the Web server nginx is running and serving content through port 8080 on all of the compromised systems. The botnet operators are registering systems under new names, since DNS providers have deleted more than 100 host names from their databases to combat the attacks.

<http://www.h-online.com/security/Botnet-discovered-on-Linux-servers--/news/114225>

### **Joe Wilson's Payments Provider Reports DDoS Attack**

BY: PETE CASHMORE, MASHABLE

09/12/2009

The online payment site Piryx claims it was targeted in recent distributed denial-of-service attacks because it hosts the fundraising campaign for Joe Wilson, who recently made headlines by screaming "You Lie!" during a health care reform speech from President Barack Obama. Piryx explains that they began to see an increase in bandwidth on their server Sept. 11. The company's bandwidth and packet rate threshold monitors were set off, and the site "saw both traditional DOS bandwidth based attacks as well as very high packet rate, low bandwidth ICMP floods."

<http://mashable.com/2009/09/12/joe-wilson-ddos/>



### **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 TACTICS AND DEFENSE

### **Raytheon Hires Air Force Network Operations Expert for Cybersecurity Post**

PRNEWswire  
09/22/2009

Raytheon has announced that they have hired retired Air Force Col. Ward Heinke as director of cyber defense solutions for its Information Security Solutions (ISS) business. Steve Hawkins, vice president of ISS at Raytheon, says that Heinke's experience in network operations and crisis communication will be an asset to Raytheon. As the commander of the 608th Air Force Network Operations Center, Heinke was responsible for coordinating and implementing "combatant commander requests for computer network operations forces and effects."

<http://news.prnewswire.com/DisplayReleaseContent.aspx?ACCT=104&STORY=/www/story/09-22-2009/0005098403&EDATE>

### **Cisco Forms Smart Grid Ecosystem**

BY: JIM DUFFY, NETWORK WORLD  
09/18/2009

Cisco recently announced the creation of the Cisco Smart Grid Ecosystem that will help accelerate the adoption of IP for utility communications networks. Members of the ecosystem include system integrators, technology vendors, power and utility integrators, service providers and other vendors from various sections of the smart grid infrastructure. Cisco has also formed a Smart Grid Technical Advisory Board which is made up of utility and energy companies from around the world, and helps Cisco to "align its product direction to customers' requirements."

<http://news.techworld.com/data-centre/3202239/cisco-forms-smart-grid-ecosystem/>

### **Microsoft to Offer Free Antivirus Software**

BY: GREGG KEIZER, COMPUTERWORLD  
09/21/2009

Microsoft recently announced that their new Microsoft Security Essentials antivirus software would "ship in the coming weeks" after issuing the beta of Security Essentials to almost 75,000 users. Microsoft says that the new antivirus and anti-spyware product uses less memory and disk space than commercial security suites from Symantec or McAfee. Microsoft has also said that users that do not have genuine copies of Windows will not be able to download Security Essentials.

<http://news.techworld.com/security/3202337/microsoft-to-offer-free-antivirus-software>

### **New Service Certifies Security of Printers, Copiers, Other Networked Devices**

BY: TIM WILSON, DARK READING  
09/21/2009

ISCA Labs, an independent division of Verizon Business, recently launched security certification and assessment services that allow vendors and enterprises to test the security of "nonmainstream networked devices" including printers, copiers, security cameras and point-of-sale systems. ISCA Labs also offers a vendor certification program and assessment service for devices that are not part of a network's infrastructure, including ATM machines, digital signs and proximity readers. George Japak, managing director at ISCA Labs, explains that the number of networked devices is increasing; any of those devices could allow hackers into a network or cause compliance issues with PCI or HIPAA standards.

<http://www.darkreading.com/securityservices/security/perimeter/showArticle.jhtml?articleID=220100424>



### **IETF Forges Botnet Clean-Up Standard**

BY: JOHN LEYDEN, THE REGISTER  
09/17/2009

The IETF recently released a draft standard – Recommendations for the Remediation of Bots in ISP Networks – which covers techniques for identifying machines that are compromised by botnet infections, how to notify affected customers and the best way to clean up infections. The document also covers how to direct users towards infection clean-up portals which contain virus information and disinfection tools. The initiative does not cover the financial costs of cleaning up an infected machine, and also does not cover possible punishments for users who leave their machines infected after they are notified.  
[http://www.theregister.co.uk/2009/09/17/ietf\\_botnet\\_clean\\_up/](http://www.theregister.co.uk/2009/09/17/ietf_botnet_clean_up/)

### **Google + reCAPTCHA Could Raise Bar in Anti-Bot, Anti-Spam Fight**

BY: RYAN NARAIN, THREATPOST  
09/16/2009

Google has announced a deal to acquire reCAPTCHA, a company that provides the distorted words at login screens. ReCAPTCHA would allow Google to “raise the bar significantly in the fight against bots and spam” since it is virtually impossible for botnets to read the CAPTCHAs. Words used by the ReCAPTCHA service come from scanned printed material and, because Google has the best

computer-vision techniques, Google will present CAPTCHA words that are even more difficult for botnets to defeat.

<http://www.threatpost.com/blogs/google-recaptcha-could-raise-bar-anti-bot-anti-spam-fight-116>

### **Heartland CEO: Credit Card Encryption Needed**

BY: GRANT GROSS, COMPUTERWORLD  
09/14/2009

Robert Carr, CEO and chairman of Heartland Payment Systems, recently told a U.S. Senate committee that credit card vendors, payment processors and retailers need to adopt encryption standards that would protect credit card numbers during online transactions.

Heartland is pushing for an end-to-end encryption standard, and is deploying tamper-resistant point-of-sale terminals at its member retailers. Heartland has also asked credit card companies to accept encrypted transactions and has helped to form an information-sharing council or payment processors. The senators asked Carr questions about the Heartland breach that was discovered in 2008, and Carr said that they still do not know the extent of the breach at this point.

[http://www.computerworld.com/s/article/9138008/Heartland\\_CEO\\_Credit\\_card\\_encryption\\_needed](http://www.computerworld.com/s/article/9138008/Heartland_CEO_Credit_card_encryption_needed)

# 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.



### **NRC, FERC to Cooperate on Cybersecurity for Nuke Plants**

BY: BEN BAIN, FEDERAL COMPUTER WEEK  
09/11/2009

The Nuclear Regulatory Commission (NRC) and the Federal Energy Regulatory Commission (FERC) have announced that they will work together to “ensure the reliability of the electric power grid and nuclear power plants.” The agreement includes developing protocols for how information about the electric grid will be shared, particularly during emergencies. The agreement was signed by R.W. Borchardt, NRC’s executive director for operations, Aug. 21 and by James Pederson, FERC chief of staff Sept. 2. <http://fcw.com/articles/2009/09/10/web-ferc-nrc-mou.aspx>

### **Cybercrime Fighters Adopt Community Tactics**

BY: JART ARMIN, INTERNET EVOLUTION  
09/10/2009

This article discusses how Internet users are being asked to do more to help prevent cyber attacks. The FBI, for example, is asking for information online about hackers, and Symantec is asking their users to log intrusions which can be analyzed to track down hackers. Symantec also plans to offer cash rewards beginning next year for information that leads to an arrest of a cyber criminal. The article discusses how this user participation could help

to develop a “Netizen-based Cyber Corps.” The article says that these changes show a “sea change with regard to community involvement” which could lead to “better security all across the Internet.”

[http://www.internetevolution.com/author.asp?section\\_id=717&doc\\_id=181555](http://www.internetevolution.com/author.asp?section_id=717&doc_id=181555)

### **Symantec Tool Calculates Your Data’s Value to Thieves**

BY: ELINOR MILLS, CNET NEWS  
09/10/2009

Symantec recently launched its Norton Online Risk Calculator – a tool that people can use to estimate how much their online information would cost on the black market. The tool can also provide a risk rating that is based on demographics, online activity and estimated value of online information. This article says that many people would be shocked at how little their sensitive personal information would cost for a criminal. A recent report from Microsoft Research says that the stolen information for sale in underground IRC channels is difficult to monetize because of all of the con artists present. Symantec hopes that their new tool will raise awareness about online theft risks and encourage consumers to use more than just an antivirus program.

[http://news.cnet.com/8301-27080\\_3-10258549-245.html](http://news.cnet.com/8301-27080_3-10258549-245.html)



### **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 - LEGAL

### **GOP Senators Move to Stop Obama Net Neutrality Rules**

BY: RYAN SINGEL, WIRED BLOG NETWORK  
09/21/2009

Senator Kay Bailey Hutchinson (R-Texas) introduced legislation Sept. 21 that would block President Barack Obama from imposing formal net neutrality rules. The rules guarantee citizens that they could use any devices, services and applications, and that ISPs cannot discriminate against services. Hutchinson says that the new rules would “suffocate Internet innovation.” Supporters of the new rules say that Hutchinson seems to be in favor of “net neutrality” as her press release defines net neutrality as policies that help to keep the Internet an “open platform for innovation and economic growth, while discouraging intentional discrimination against particular content or applications.”

<http://www.wired.com/epicenter/2009/09/rep-ublican-net-neutrality-amendment/>

### **Republicans to Push Against Net Neutrality; FCC Says Start of Process**

BY: CECILIA KANG, WASHINGTON POST  
09/21/2009

Senate Republicans oppose the FCC’s new rules on net neutrality, and have added an amendment to the Interior Appropriations bill that would stop funding at the agency for new regulatory mandates. The amendment is unlikely to be approved in the Democrat-majority Congress though. Senator Kay Bailey Hutchinson (R-Texas) says that the FCC’s regulations could “stifle investment incentives.” FCC Chairman Julius Genachowski says that critics of the new regulations have drawn conclusions prematurely about how consumers and businesses are being affected by current Web policies.

[http://voices.washingtonpost.com/posttech/2009/09/senate\\_republicans\\_to\\_push\\_aga.html](http://voices.washingtonpost.com/posttech/2009/09/senate_republicans_to_push_aga.html)

### **Presidential Internet Kill Switch May Still be Alive**

BY: ROY MARK, EWEEK.COM  
09/20/2009

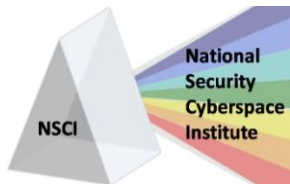
Senators Jay Rockefeller and Olympia Snowe introduced the Cybersecurity Bill of 2009 in April. The bill has received much criticism due to the provision that would allow the president the authority to shut down the Internet in case of a national crisis. The bill has since been redrafted, but the provision that gives the president an “Internet kill switch” was not removed from the bill. The new version of the cybersecurity bill says that the president would “direct the national response to the cyber-threat” in case of a cybersecurity emergency, and that the president decides what is critical infrastructure in government and private networks.

<http://www.eweek.com/prestitial.php?type=rest&url=http%3A%2F%2Fwww.eweek.com%2F%2Fa%2FSecurity%2FPresidential-Internet-Kill-Switch-May-Still-Be-Alive-577445%2F&ref=>

### **Intelligence Analyst Says Hacking Charge Doesn’t Compute**

BY: KEVIN POULSEN, WIRED BLOG NETWORK  
09/18/2009

Brian Keith Montgomery, a Defense Department intelligence analyst, is being charged with federal computer hacking after a password used in a nationwide terrorism investigation was accidentally sent to tens of thousands of analysts that did not have the need-to-know. Montgomery was working on a covert program at the National Geospatial Intelligence Agency, and held a top secret clearance when he received a message with the password and another message that included details about an unrelated classified operation. Montgomery used the password to log into a system used in the terrorism investigation.



Federal prosecutors in Virginia charged Montgomery Sept. 11 with a felony count of gaining unauthorized access to a protected computer, but Montgomery argues that he did not notice a message saying that he was not authorized to access the system, and says that he should not be prosecuted as a criminal for using a password that was widely distributed. [http://www.wired.com/threatlevel/2009/09/montgomery\\_defense/](http://www.wired.com/threatlevel/2009/09/montgomery_defense/)

### **Cybersecurity Measure Takes A Back Seat for Co-Sponsors**

BY: ANDREW NOYES, CONGRESSDAILY  
09/17/2009

The hearing for the controversial cybersecurity legislation from Senators John Rockefeller and Sen. Olympia Snowe will probably be postponed until next month, as aids retool key provisions in the bill, and while the bill's co-sponsors focus on the healthcare debate. A forthcoming version of the bill will likely include details on how the president and government and industry officials can work to develop an emergency response plan for cyber events. The final bill will most likely not include a definition of an "Internet emergency" and Rockefeller's team says that other panels, such as the Senate Homeland Security and Governmental Affairs Committee, are also preparing bills. [http://www.nextgov.com/nextgov/ng\\_20090917\\_5619.php](http://www.nextgov.com/nextgov/ng_20090917_5619.php)

### **Cerf: Turning Off Pieces of the Internet 'not sensible' as Security Strategy**

BY: PAUL KRILL, INFOWORLD  
09/17/2009

In this article, InfoWar Editor at Large Paul Krill interviews Vinton Cerf, co-designer of the basic architecture of the Internet and of the TCP/IP protocol, on various topics including government legislation that would give the president authority over the Internet. Cerf says that giving the president the authority to shut down the Internet is "not sensible," but that focusing attention on Internet security is a good thing. Cerf also says that the motivation behind the Snowe-Rockefeller legislation was to bring attention to our dependence on the Internet and the potential from criminals to use that dependence against us.

<http://www.infoworld.com/t/internet/cerf-turning-pieces-internet-not-sensible-security-strategy-252>

### **Trial Set for 'Botnet for Hire' Duo**

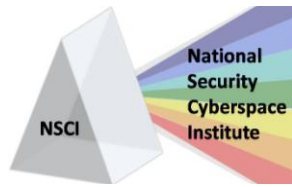
BY: DAN GOODIN, THE REGISTER  
09/16/2009

The trial of Thomas James Frederick Smith and David Anthony Edwards, indicted in April on a single count of conspiracy to intentionally cause damage to a protected computer, is scheduled to begin Nov. 16. The men developed botnet software – Nettick – and advertised the services online, telling one customer they had infected almost 22,000 computers with the malware. In August 2006, the men used a portion of their botnet to carry out a DDoS attack on an IP address to sell the botnet.

[http://www.theregister.co.uk/2009/09/16/both\\_order\\_trial\\_set/](http://www.theregister.co.uk/2009/09/16/both_order_trial_set/)



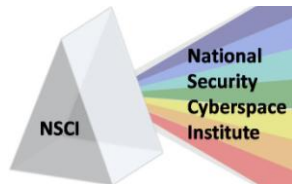
Alion is a progressive employee-owned research, management and technology company with worldwide government and commercial capabilities supporting complex programs including network and information security, M&S, experimentation, testing and Risk / Vulnerability tools.



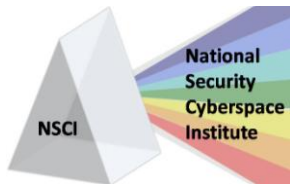
## CYBERSPACE-RELATED CONFERENCES

**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](#).

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>
30 Sep – 1 Oct 2009	<b>New England Information Security Forum</b> , Boston, MA; <a href="https://www.isc2.org/EventDetails.aspx?id=5064">https://www.isc2.org/EventDetails.aspx?id=5064</a>
30 Sep – 2 Oct 2009	<b>The 1st International ICST Conference on Digital Forensics &amp; Cyber Crime</b> , Albany, NY; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1m0hxx">http://www.conferencealerts.com/seeconf.mv?q=ca1m0hxx</a>
6 Oct 2009	<b>Cyber Security Conference – A Shared Responsibility</b> , John Hopkins APL - Kossiakoff Conference and Education Center, Maryland, <a href="https://www.fbcinc.com/csc/default.aspx">https://www.fbcinc.com/csc/default.aspx</a>
6 Oct 2009	<b>SecureIndianapolis</b> , Carmel, IN; <a href="https://www.isc2.org/EventDetails.aspx?id=4082&amp;display=eventdetails&amp;origin=">https://www.isc2.org/EventDetails.aspx?id=4082&amp;display=eventdetails&amp;origin=</a>
6 – 8 Oct 2009	<b>Information Security Solutions Europe Conference (ISSE 2009)</b> , The Hague, The Netherlands; <a href="https://www.isc2.org/EventDetails.aspx?id=3826">https://www.isc2.org/EventDetails.aspx?id=3826</a>
13 Oct 2009	<b>SecureLondon 2009</b> , London, UK; <a href="https://www.isc2.org/EventDetails.aspx?id=3812&amp;display=eventdetails&amp;origin=">https://www.isc2.org/EventDetails.aspx?id=3812&amp;display=eventdetails&amp;origin=</a>
13 – 14 Oct 2009	<b>SC World Congress Enterprise Data Security Conference and Expo 2009</b> , New York, NY; <a href="http://www.scmagazineus.com/SC-World-Congress-2009/section/886/">http://www.scmagazineus.com/SC-World-Congress-2009/section/886/</a>
15 Oct 2009	<b>SecureBaltimore</b> , Baltimore, MD; <a href="https://www.isc2.org/EventDetails.aspx?id=5084&amp;display=eventdetails&amp;origin=">https://www.isc2.org/EventDetails.aspx?id=5084&amp;display=eventdetails&amp;origin=</a>
15 Oct 2009	<b>2<sup>nd</sup> Annual Cybersecurity Expo</b> , Memphis, TN; <a href="http://cyberexpo.memphis.edu/">http://cyberexpo.memphis.edu/</a>
19 – 22 Oct 2009	<b>2009 Control Systems Cyber Security Conference</b> , Bethesda, MD; <a href="http://realtimeacs.com/?page_id=38">http://realtimeacs.com/?page_id=38</a>
20 Oct 2009	<b>SecureSouthernCalifornia</b> , Marina Del Rey, CA; <a href="https://www.isc2.org/EventDetails.aspx?id=4074&amp;display=eventdetails&amp;origin=">https://www.isc2.org/EventDetails.aspx?id=4074&amp;display=eventdetails&amp;origin=</a>
20 – 22 Oct 2009	<b>RSA Conference – London 2009</b> , London, UK; <a href="https://www.isc2.org/EventDetails.aspx?id=4440">https://www.isc2.org/EventDetails.aspx?id=4440</a>
20 – 22 Oct 2009	<b>The 3<sup>rd</sup> International Conference on Cyberlaw</b> , Beirut, Lebanon; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1mxx6m">http://www.conferencealerts.com/seeconf.mv?q=ca1mxx6m</a>
22 – 24 Oct 2009	<b>Tech-It-Up International 2009</b> , Kamloops, British Columbia, Canada; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1mhim6">http://www.conferencealerts.com/seeconf.mv?q=ca1mhim6</a>
23 – 24 Oct 2009	<b>Evidence in the Information Age: A National Symposium on the Collection, Analysis and Legal Applications of Digital Evidence</b> , Pittsburgh, PA; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1mxm33">http://www.conferencealerts.com/seeconf.mv?q=ca1mxm33</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>
2 – 3 Nov 2009	<b>Midwest Information Security Forum</b> , Chicago, IL; <a href="https://www.isc2.org/EventDetails.aspx?id=5066">https://www.isc2.org/EventDetails.aspx?id=5066</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>
8 Nov 2009	<b>SecureMuscat</b> , Muscat, Oman; <a href="https://www.isc2.org/EventDetails.aspx?id=4150&amp;display=eventdetails&amp;origin=">https://www.isc2.org/EventDetails.aspx?id=4150&amp;display=eventdetails&amp;origin=</a>
11 Nov 2009	<b>The Security 500 Conference</b> , New York, NY; <a href="http://www.securingenewground.com/Security500/default2.htm">http://www.securingenewground.com/Security500/default2.htm</a>



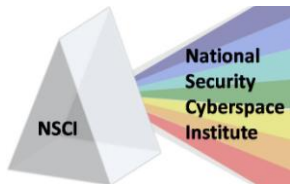
12 Nov 2009	<b>SecureSydney</b> , Sydney, Australia; <a href="https://www.isc2.org/EventDetails.aspx?id=4982">https://www.isc2.org/EventDetails.aspx?id=4982</a>
12 Nov 2009	<b>SecureHouston</b> , Houston, TX; <a href="https://www.isc2.org/EventDetails.aspx?id=4086">https://www.isc2.org/EventDetails.aspx?id=4086</a>
16 – 18 Nov 2009	<b>Cyber Security for National Defense</b> , Washington DC; <a href="http://www.cybersecurityevent.com/Event.aspx?id=211620">http://www.cybersecurityevent.com/Event.aspx?id=211620</a>
17 – 19 Nov 2009	<b>PDCO9</b> , Los Angeles, CA; <a href="https://www.isc2.org/EventDetails.aspx?id=5050">https://www.isc2.org/EventDetails.aspx?id=5050</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>
28 Nov – 6 Dec 2009	<b>SANS London 2009</b> , London, UK; <a href="https://www.isc2.org/EventDetails.aspx?id=5078">https://www.isc2.org/EventDetails.aspx?id=5078</a>
3 Dec 2009	<b>SecureCharlotte</b> , Charlotte, NC; <a href="https://www.isc2.org/EventDetails.aspx?id=4600">https://www.isc2.org/EventDetails.aspx?id=4600</a>
8 – 9 Dec 2009	<b>Pacific Information Security Forum</b> , San Francisco, CA; <a href="https://www.isc2.org/EventDetails.aspx?id=5068">https://www.isc2.org/EventDetails.aspx?id=5068</a>
11 – 18 Dec 2009	<b>SANS Cyber Defense Initiative 2009</b> , Washington DC; <a href="http://www.sans.org/cyber-defense-initiative-2009/?utm_source=offsite&amp;utm_medium=misc&amp;utm_content=20090725_te_072509_cdi09_allconf&amp;utm_campaign=CDI_East_2009&amp;ref=46324">http://www.sans.org/cyber-defense-initiative-2009/?utm_source=offsite&amp;utm_medium=misc&amp;utm_content=20090725_te_072509_cdi09_allconf&amp;utm_campaign=CDI_East_2009&amp;ref=46324</a>
27 – 28 Jan 2010	<b>Cyber Warfare 2010</b> , London, UK; <a href="http://www.cyberwarfare-event.com/Event.aspx?id=228104">http://www.cyberwarfare-event.com/Event.aspx?id=228104</a>
17 – 18 Feb 2010	<b>7<sup>th</sup> Annual Worldwide Security Conference</b> , Brussels, Belgium; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1m3m8x">http://www.conferencealerts.com/seeconf.mv?q=ca1m3m8x</a>
12 – 14 Mar 2010	<b>5<sup>th</sup> Global Conference: Cybercultures – Exploring Critical Issues</b> , Salzburg, Austria; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1mx666">http://www.conferencealerts.com/seeconf.mv?q=ca1mx666</a>
18 – 19 Mar 2010	<b>Cyber Security - Legal and Policy Issues for National Security, Law Enforcement and Private Industry</b> , San Antonio, TX; <a href="http://www.stmarytx.edu/ctl/index.php?site=centerForTerrorismLawCyberSecurity">http://www.stmarytx.edu/ctl/index.php?site=centerForTerrorismLawCyberSecurity</a>
8 – 9 April 2010	<b>5<sup>th</sup> International Conference on Information Warfare and Security</b> , Wright-Patterson Air Force Base, Ohio; <a href="http://academic-conferences.org/iciw/iciw2010/iciw10-home.htm">http://academic-conferences.org/iciw/iciw2010/iciw10-home.htm</a>
23 April 2010	<b>Social Networking in Cyberspace</b> , Wolverhampton, UK; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1mhm38">http://www.conferencealerts.com/seeconf.mv?q=ca1mhm38</a>
17 July 2010	<b>Cyberpsychology and Computing Psychology Conference (CyComp 2010)</b> , Bolton, Lancashire, UK; <a href="http://www.conferencealerts.com/seeconf.mv?q=ca1mxia6">http://www.conferencealerts.com/seeconf.mv?q=ca1mxia6</a>



## CYBERSPACE-RELATED TRAINING COURSES

**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](#).

<b>Certified Ethical Hacker</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=10463&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=10463&amp;catid=191&amp;country=United+States</a>
<b>Certified Secure Programmer (ECSP)</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/ECSP.htm">http://www.eccouncil.org/Course-Outline/ECSP.htm</a>
<b>Certified VoIP Professional</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/ECVP.htm">http://www.eccouncil.org/Course-Outline/ECVP.htm</a>
<b>CISA Prep Course</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9416&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9416&amp;catid=191&amp;country=United+States</a>
<b>CISM Prep Course</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9877&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9877&amp;catid=191&amp;country=United+States</a>
<b>CISSP Prep Course</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=8029&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=8029&amp;catid=191&amp;country=United+States</a>
<b>Computer Hacking Forensic Investigator</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/CHF1%20Course.htm">http://www.eccouncil.org/Course-Outline/CHF1%20Course.htm</a>
<b>Contingency Planning</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11919&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11919&amp;catid=191&amp;country=United+States</a>
<b>Cyber Law</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/CyberLaw%20Course.htm">http://www.eccouncil.org/Course-Outline/CyberLaw%20Course.htm</a>
<b>Defending Windows Networks</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=10836&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=10836&amp;catid=191&amp;country=United+States</a>
<b>DIACAP – Certification and Accreditation Process</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11776&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11776&amp;catid=191&amp;country=United+States</a>
<b>DIACAP – Certification and Accreditation Process, Executive Overview</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11778&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11778&amp;catid=191&amp;country=United+States</a>
<b>Disaster Recovery</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/Disaster%20Recovery%20Course.htm">http://www.eccouncil.org/Course-Outline/Disaster%20Recovery%20Course.htm</a>
<b>E-Business Security</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/e-Security%20Course.htm">http://www.eccouncil.org/Course-Outline/e-Security%20Course.htm</a>
<b>E-Commerce Architect</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/E-Commerce%20Architect%20Course.htm">http://www.eccouncil.org/Course-Outline/E-Commerce%20Architect%20Course.htm</a>
<b>ESCA/LPT</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/ECSA-LPT-Course.htm">http://www.eccouncil.org/Course-Outline/ECSA-LPT-Course.htm</a>
<b>Ethical Hacking and Countermeasures</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/Ethical%20Hacking%20and%20Countermeasures%20Course.htm">http://www.eccouncil.org/Course-Outline/Ethical%20Hacking%20and%20Countermeasures%20Course.htm</a>



<b>Foundstone Ultimate Hacking</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=978&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=978&amp;catid=191&amp;country=United+States</a>
<b>Foundstone Ultimate Hacking Expert</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=7938&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=7938&amp;catid=191&amp;country=United+States</a>
<b>Foundstone Ultimate Web Hacking</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=979&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=979&amp;catid=191&amp;country=United+States</a>
<b>INFOSEC Certification and Accreditation Basics</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11905&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11905&amp;catid=191&amp;country=United+States</a>
<b>INFOSEC Forensics</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11943&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11943&amp;catid=191&amp;country=United+States</a>
<b>INFOSEC Strategic Planning</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11933&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11933&amp;catid=191&amp;country=United+States</a>
<b>Linux Security</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/Linux%20Security%20Course.htm">http://www.eccouncil.org/Course-Outline/Linux%20Security%20Course.htm</a>
<b>Mandiant Incident Response</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/wwwsearch.asp?country=United+States&amp;keyword=9806">http://www.globalknowledge.com/training/wwwsearch.asp?country=United+States&amp;keyword=9806</a>
<b>Network Management</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11937&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11937&amp;catid=191&amp;country=United+States</a>
<b>Network Security Administrator (ENSA)</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/ENSA.htm">http://www.eccouncil.org/Course-Outline/ENSA.htm</a>
<b>Network Vulnerability Assessment Tools</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11784&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11784&amp;catid=191&amp;country=United+States</a>
<b>NIST 800-37 - Security Certification and Accreditation of Federal Information Systems</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11780&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11780&amp;catid=191&amp;country=United+States</a>
<b>NIST 800-37 - Security Certification and Accreditation of Federal Information Systems - Executive Overview</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11782&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11782&amp;catid=191&amp;country=United+States</a>
<b>Policy and Procedure Development</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11923&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11923&amp;catid=191&amp;country=United+States</a>
<b>Project Management in IT Security</b>	EC-Council, Online, <a href="http://www.eccouncil.org/Course-Outline/Project%20Management%20in%20IT%20Security%20Course%20Outline/Project%20Management%20in%20IT%20Security%20Course%20Outline.html">http://www.eccouncil.org/Course-Outline/Project%20Management%20in%20IT%20Security%20Course%20Outline/Project%20Management%20in%20IT%20Security%20Course%20Outline.html</a>
<b>Red Hat Enterprise Security: Network Services</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=7972&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=7972&amp;catid=191&amp;country=United+States</a>



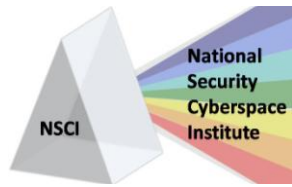
## Keeping Cyberspace Professionals Informed

<b>Risk Analysis and Management</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11913&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11913&amp;catid=191&amp;country=United+States</a>
<b>Security Certified Network Architect</b>	Security Certified Program, Self-Study, <a href="http://www.securitycertified.net/getdoc/ac8d836b-cb21-4a87-8a34-4837e69900c6/SCNA.aspx">http://www.securitycertified.net/getdoc/ac8d836b-cb21-4a87-8a34-4837e69900c6/SCNA.aspx</a>
<b>Security Certified Network Professional</b>	Security Certified Program, Self-Study, <a href="http://www.securitycertified.net/getdoc/6e1aea03-2b53-487e-bab6-86e3321cb5bc/SNCP.aspx">http://www.securitycertified.net/getdoc/6e1aea03-2b53-487e-bab6-86e3321cb5bc/SNCP.aspx</a>
<b>Security Certified Network Specialist</b>	Security Certified Program, Self-Study, <a href="http://www.securitycertified.net/getdoc/f6d07ac4-abc2-4306-a541-19f050f32683/SCNS.aspx">http://www.securitycertified.net/getdoc/f6d07ac4-abc2-4306-a541-19f050f32683/SCNS.aspx</a>
<b>Security for Non-security Professionals</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=8461&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=8461&amp;catid=191&amp;country=United+States</a>
<b>SSCP Prep Course</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9876&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=9876&amp;catid=191&amp;country=United+States</a>
<b>Vulnerability Management</b>	Global Knowledge, Dates and Locations: <a href="http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11941&amp;catid=191&amp;country=United+States">http://www.globalknowledge.com/training/course.asp?pageid=9&amp;courseid=11941&amp;catid=191&amp;country=United+States</a>

### CYBER BUSINESS DEVELOPMENT OPPORTUNITIES

**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](#).

Office	Title	Link
DLA Acquisition Locations	Information Technology (IT) Information Assurance Support and Management Services, Defense Distribution Center (DDC)	<a href="https://www.fbo.gov/spg/DLA/J3/DDC/SP3300-09-R-0046/listing.html">https://www.fbo.gov/spg/DLA/J3/DDC/SP3300-09-R-0046/listing.html</a>
Procurement Directorate	DoD DMZ Engineering Support	<a href="https://www.fbo.gov/spg/DISA/D4AD/DITCO/RFICBest/listing.html">https://www.fbo.gov/spg/DISA/D4AD/DITCO/RFICBest/listing.html</a>
Procurement Directorate	DISA Implementation of Web Audit Log Collection and Analysis Tools	<a href="https://www.fbo.gov/spg/DISA/D4AD/DITCO/DISAWEBAUDIT/listing.html">https://www.fbo.gov/spg/DISA/D4AD/DITCO/DISAWEBAUDIT/listing.html</a>
PEO STRICOM	D--Threat Computer Network Operation (CNO) Teams for Test and Evaluation events	<a href="https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=d713ee539a271238c8580dd6042731ea&amp;tab=core&amp;_cview=0">https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=d713ee539a271238c8580dd6042731ea&amp;tab=core&amp;_cview=0</a>
Department of the Air Force	A+, Network+, Security+ Training and Certification	<a href="https://www.fbo.gov/spg/USAF/ACC/99CONS/F3G3FA9167AC02/listing.html">https://www.fbo.gov/spg/USAF/ACC/99CONS/F3G3FA9167AC02/listing.html</a>
Department of the Air Force	D -- AIR FORCE SYSTEMS NETWORK	<a href="https://www.fbo.gov/spg/USAF/AFMC/ESC/R2249/listing.html">https://www.fbo.gov/spg/USAF/AFMC/ESC/R2249/listing.html</a>
Air Force Materiel Command	Integrated Cyber Defense & Support Technologies	<a href="https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=cd045a392c920683ccb0b03df09bb134&amp;tab=core&amp;_cview=1">https://www.fbo.gov/index?s=opportunity&amp;mode=form&amp;id=cd045a392c920683ccb0b03df09bb134&amp;tab=core&amp;_cview=1</a>



Air Force Materiel Command	Cyber Command and Control (C2) Technologies	<a href="https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA0809-RIKA/listing.html">https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA0809-RIKA/listing.html</a>
Air Force Materiel Command	USAF Electronic Warfare Battle Management Technology CRFI	<a href="https://www.fbo.gov/spg/USAF/AFMC/ASC/USAF_Electronic_Warfare_Battle_Management_Technology/listing.html">https://www.fbo.gov/spg/USAF/AFMC/ASC/USAF Electronic Warfare Battle Management Technology/listing.html</a>
Air Force Materiel Command	CompTIA Security+ Training	<a href="https://www.fbo.gov/spg/USAF/AFMC/88CONS/FA8601-09-T-0049/listing.html">https://www.fbo.gov/spg/USAF/AFMC/88CONS/FA8601-09-T-0049/listing.html</a>
Air Force Materiel Command	Military Communications and Surveillance Technologies and Techniques	<a href="https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA-09-09-RIKA/listing.html">https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA-09-09-RIKA/listing.html</a>
Air Force Materiel Command	CyberSoft VFind Security Tool Kit Maintenance & Support	<a href="https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/FA8751-09-Q-0379/listing.html">https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/FA8751-09-Q-0379/listing.html</a>
Air Force Materiel Command	Provide Information Awareness (IA) training	<a href="https://www.fbo.gov/spg/USAF/AFMC/75/F2DC/CR9180A001/listing.html">https://www.fbo.gov/spg/USAF/AFMC/75/F2DC/CR9180A001/listing.html</a>
Air Force Materiel Command	D – NETCENTS-2 Netops and Infrastructure Solutions	<a href="https://www.fbo.gov/spg/USAF/AFMC/ESC/FA8771-09-R-0018/listing.html">https://www.fbo.gov/spg/USAF/AFMC/ESC/FA8771-09-R-0018/listing.html</a>
Air Force Materiel Command	D – NETCENTS-2 NETOPS and Infrastructure Solutions (Small Business Companion)	<a href="https://www.fbo.gov/spg/USAF/AFMC/ESC/FA8771-09-R-0019/listing.html">https://www.fbo.gov/spg/USAF/AFMC/ESC/FA8771-09-R-0019/listing.html</a>
Air Force Materiel Command	Security Certificate & Accreditation Services for Information Systems	<a href="https://www.fbo.gov/spg/USAF/AFMC/75/FA8201-09-R-0088/listing.html">https://www.fbo.gov/spg/USAF/AFMC/75/FA8201-09-R-0088/listing.html</a>
Air Combat Command	A+, Network+, Security+ Training and Certification	<a href="https://www.fbo.gov/spg/USAF/ACC/99CONS/F3G3FA9167AC02/listing.html">https://www.fbo.gov/spg/USAF/ACC/99CONS/F3G3FA9167AC02/listing.html</a>
United States Marine Corps	R--Internet Monitoring Services	<a href="https://www.fbo.gov/spg/DON/USMC/M67004/M6700409T0108/listing.html">https://www.fbo.gov/spg/DON/USMC/M67004/M6700409T0108/listing.html</a>
Bureau of Industry & Security	International Competitive Bidding (ICB): Implementation and Support of NATO Enterprise	<a href="https://www.fbo.gov/spg/DOC/BIS/comp99/IFB-CO-12870-NEDS/listing.html">https://www.fbo.gov/spg/DOC/BIS/comp99/IFB-CO-12870-NEDS/listing.html</a>
Department of the Army	D--Information Assurance, Engineering System Solutions Development, Testing, Deployment and Life Cycle Support	<a href="https://www.fbo.gov/spg/USA/DABL/DABL01/W91QUZ-09-0000/listing.html">https://www.fbo.gov/spg/USA/DABL/DABL01/W91QUZ-09-0000/listing.html</a>
Business Transformation Agency	Sources sought or request for information (RFI), DoD Information Assurance (IA) Controls (For Information Purposes Only)	<a href="https://www.fbo.gov/spg/ODA/BTA/BTA-BMD/HQ0566-09-InformationAssurance/listing.html">https://www.fbo.gov/spg/ODA/BTA/BTA-BMD/HQ0566-09-InformationAssurance/listing.html</a>
National Aeronautics and Space Administration	U--CISSP CERTIFICATION EDUCATION	<a href="https://www.fbo.gov/spg/NASA/GRC/OPDC2020/NNC09306220Q/listing.html">https://www.fbo.gov/spg/NASA/GRC/OPDC2020/NNC09306220Q/listing.html</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>Chief Operations Officer <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.**