



Issue 16, March 24, 2009

E-Telligence

2009 Event Calendar

- April 13-16, 2009
Cyber Physical Systems Week
San Francisco, CA, USA
[Click here](#)
- April 20-24, 2009
18th Annual International World Wide Web Conference
Madrid, Spain
[Click here](#)
- April 27-29, 2009
Critical Infrastructure and Security Risk Vulnerability Workshop
Vancouver, BC, Canada
[Click here](#)
- May 12-14, 2009
APWG Spring Counter-eCrime Operations Summit
Barcelona, Spain
[Click here](#)
- May 20, 2009
GeoSpatial Summit
Schenectady, NY, USA
[Click here](#)
- June 3-4, 2009
12th Annual New York State Cyber Security Conference
Albany, NY, USA
[Click here](#)
- June 9-11, 2009
Kestenberg Siegal Lipkus LLP Anti-Counterfeiting Training Conference
Vancouver, BC Canada
[Click here](#)
- June 18-19, 2009
Tri-Lateral Security Conference
Calgary, AB, Canada
[Click here](#)
- July 10-12, 2009
Video Game Cultures and Future of Interactive Entertainment Conference
Mansfield College, Oxford, UK
[Click here](#)

HEADLINE NEWS — March 24, 2009

What's New on the Frontline!

Pelgrin Receives Cybercrime Fighter Award

March 18, 2009 — William Pelgrin, director of the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) and chair of the Multi-State Information Sharing and Analysis Center (MS-ISAC), was recently presented with the McAfee Cybercrime Fighter Award.



Mr. Will Pelgrin, on right, receiving McAfee Cybercrime Fighter Award from Mr. Dave DeWalt, President and CEO of McAfee Inc.

The award is given to an individual from government, industry, academia or a non-governmental organization who has exemplified outstanding leadership in the global effort to combat cyber crime. Pelgrin was recognized for his cyber security leadership within New York State as well as nationally through the MS-ISAC.

Experts See Shortfall in Cybersecurity Research

InternetNews.com (03/19/09); Corbin, Kenneth — The United States is not prepared to deal with the emerging threats against the country's digital infrastructure, warned cyber security experts at a recent U.S. Senate Commerce Committee meeting. The experts also said that Congress needs to make information security and security education a bigger priority. "The simplest way to state this is the nation is under attack," said Purdue University professor Eugene Spafford, executive director of the Center for Education and Research in Information Assurance and Security. "It is a hostile attack, it is a continuing attack, and it has been going on for years, and we have been ignoring it."

James Lewis, director of the Center for Strategic and International Studies, said cyber attacks threaten the long-term economic competitiveness and technological leadership of the United States. Senate Commerce Committee chairman John Rockefeller (D-W.Va.) said he is encouraged by President Obama's focus on cyber security, but cautioned that time is critical as computers are increasingly being used to manage the country's infrastructure.

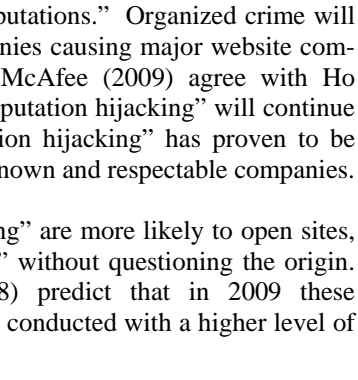
Rockefeller said he plans to introduce legislation that would boost cyber security education at the university level. Spafford said the U.S. needs more cyber security experts and noted that universities graduate just 50 to 60 Ph.D.s in fields related to cyber security. "Of those, perhaps 10 to 15 are going to return to their home countries to start businesses to compete against the U.S. because our visa policies won't let them stay," he said. [Click here](#)

Welcome to E-Telligence

Twice a month, we'll be profiling guest writers, cyber crime news and important events to keep you informed.

UNDERSTANDING CYBERCRIME IN THE NEW AGE OF VIRTUAL CRIME

By Magda Marczak, M.A., Crime Analyst, Delta Police Criminal Intelligence
Part One of Two



Cybercrime has become a significant challenge for many law enforcement agencies as traditional policing theories become obsolete in the cyber-world (Walker, Brock & Stuart, 2006).

These recent struggles have resulted in the development of a survey to determine the impact of cybercrime on Canadians, in January 2008, by the Canadian Association of Police Board (CAPB).

The results of the survey reveal that cybercrime "will soon become the number one crime in Canada" (CAPB, 2008). Computers have become a feeding ground for viruses, identity theft, web jacking and theft of computer systems. Hackers are employing phishing methods which are used to deceive financial institutions, retailers, and individuals. Although, policing cybercrime is a federal responsibility, many municipal police agencies have set up specialty units to combat the current problem (Federation of Canadian Municipalities).

Cybercrime challenges have sparked debates among police agencies to identify recommendations to combat the current problem. As a result, the focus here is to understand the definition of cybercrime and the involvement of organized crime with respect to cybercrime. Additionally, this article will also discuss the upcoming 2009 trends and provide an outline of recommendations to address the current problem of cybercrime.

Cybercrime: Definition

Literature reveals that researchers have been unable to agree on a definition of cybercrime. Gordon and Ford (2006) argue that the term cybercrime is used widespread, although most people find the term difficult to define. Cybercrime has many facets, and the definition may vary depending on the perception of the victim and the observer. For example, Thomas and Loaders (2000:3) define cybercrime as "computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks." On the other hand, in 2008, CISC National Threat Assessment – The Feature Focus Area defined cybercrime as "criminal offences conducted or enhanced through technological means, and criminal offences that would not exist without technology" (CISC National TA, 2008). Finally, Zeviar-Goose (1997-1998) suggest that the definition of cybercrime should include fraud, child pornography, unauthorized access, and cyberstalking.

Within the above mentioned definitions, cybercrime can be classified as the following: 'computer-assisted crimes' (crimes that pre-date the Internet, but have taken on a new life in cyberspace (i.e., fraud, money laundering, theft, pornography) and computer-focused crimes (those crimes that have emerged with the establishment of the Internet (i.e., hacking, viral attacks) (Furnell, 2002:22). According to Yar (2005), these classifications determine the "manner in which technology plays a role, (i.e., whether technology is a contingent (computer-assisted) or necessary (computer-focused) element in the commission of the offence (Yar, 2005:409-410).

In addition, the ability of criminals to target individuals, companies, and property has amplified because the Internet allows a single user to reach out and interact with thousands of individuals simultaneously. According to Yar (2005:411), technology has become a 'force multiplier,' since criminals require minimal resources, but may generate colossal damage to individuals and companies.

Furthermore, the Internet allows criminals to adopt false virtual identities, which is viewed as a powerful and dangerous tool since criminals can continue to commit crime while maintaining their anonymity through disguise over the Internet. This becomes a challenge for law enforcement agencies to identify the real suspect (Yar, 2005; Joseph, 2003; Snyder, 2001). One can only imagine that this challenge increases tenfold when the suspects are complex organizations, often with money and therefore experts and capabilities within their reach.

The above definitions reveal that "cybercrime" has become a new form of illicit activity because the cyberspace environment permits multiple user connectivity, anonymity and plasticity of online identity. Unfortunately, cybercrime is also known as the "invisible" crime, because precise figures on the global cost of online crimes are hard to pin down, in part because some organizations prefer to keep quiet rather than publicize that their networks have been successfully attacked (McAfee, 2009; Co-sco, 2008).

Cybercrime in 2009 and Organized Crime in BC

Cybercrime is increasingly being committed by organized crime groups out to profit from sophisticated ruses, rather than hackers keen to make an online name for themselves. An increasing proportion of these attacks are occurring from remote locations using "bot-nets" technology, which allows organized groups to control networks of computers remotely. As a result this is where the danger lies in the more anonymous virtual interlopers (McAfee, 2006).

Organized crime has been able to take advantage of vulnerabilities in networks and computers to gain access to personal identification information and financial data. For example, British Columbia is noticing an increase of organized crime groups recruiting street level drug users to commit commercial break and enter to target computer hard drives, containing customer credit card information. These groups are offering as much as \$1,000 for each hard drive.

Some businesses are targeted more than others because they do not follow the PCI standards. The PCI standards are multifaceted security standards that ensure protection for customer's information by implementing a set of policies and procedures that guide businesses how to effectively and safely store information.

These sophisticated groups are now using the Internet for extortion, fraud, money laundering, and theft. These crimes can be carried out quickly, efficiently, and with minimal risk. The Internet allows these organized groups the use of pseudonyms or online identities with anonymity and ability to move money rapidly between various bank accounts and countries.

Unfortunately, this becomes a challenge for law enforcement to follow these transactions. Cybercrime has no borders and countries have varying laws with respect to cybercrime, thus making it difficult to prosecute (McAfee, 2006).

Williams (2002) argues that organized crime on a more regular basis now hire financial specialists to conduct their money laundering transactions. These financial experts provide an extra layer of insulation to organized crime as they are knowledgeable about the layering of financial transactions and off shore financial jurisdictions. Since organized crime groups have the money to hire financial experts, there is no need for them to develop expertise about the Internet. They are able to hire experts who can carry out the tasks efficiently and effectively and results in minimal risk.

The latest article written by Vanessa Ho for eChannelline Daily News (2009) predicts that in 2009, law enforcement agencies "will see more than 80 percent of all malicious content hosted on sites with 'good' reputations." Organized crime will target large respectable companies causing major website compromises. Cisco (2008) and McAfee (2009) agree with Ho (2009), as they predict that "reputation hijacking" will continue in 2009. In essence "reputation hijacking" has proven to be effective since it targets well known and respectable companies.

Victims of "reputation hijacking" are more likely to open sites, e-mails from "associated sites" without questioning the origin. Ho (2009) and Cisco (2008) predict that in 2009 these "reputation hijackings" will be conducted with a higher level of sophistication.

McAfee 2009 Threat Prediction forecasts that because of the current economic turmoil law enforcement agencies will see an increase of malicious mirror sites of financial and banking targets. Customers and businesses will be utilizing the Internet to find attractive offers, without realizing that they are being lured by a cybercriminal. These usually take form of fake investment sites, fake financial transactions services and fake legal services.

Mohammed Akif, a security and privacy lead for Microsoft Canada argues that "organized crime is paying more attention to the Internet." In other words, they are using the Internet for more sophisticated attacks, which enables the "criminals" to steal vital information which leads to financial loss.

Web threats are on a constant rise because of the amount of annual web applications that are going online, thus creating new victims each year. Finally, the Web makes it hard to trace back to the criminal, hence allowing the continuous victimization (Ho, 2009). According to Ho (2009), in 2008 law enforcement officers identified the appearance of rogue security appliances as a more common trend. Rogue security software is an application that appears to be beneficial from a security perspective, but instead provides little or no security and attempts to lure users into participating in fraudulent transactions.

Some products defined as rogue simply fail to provide the reliable protection that a consumer paid for. Others are far more sinister, masquerading as legitimate security software, and using deceptive tactics to con users into buying the product.

Unfortunately for computer users, the number of rogue security found online is rising at ever-increasing rates, blurring the lines between legitimate software and applications that put consumers in harm's way. According to Gary McIntyre, lead architect for security service for IBM Canada rogue security applications will continue to expand in 2009 (Ho, 2009).

Additionally, Cisco in their Annual Security Report (2008) predicts that sophisticated attacks will continue in 2009. In fact, Cisco believes that the current worldwide economic crisis is enticing the criminals to target more specific groups such as individuals, business, organizations, and the government.

According to Cisco, phishing techniques have been very profitable and they will continue in 2009. The "blended" approach combining e-mail, Web-based threats, and intrusions have proven to be successful in the past and they will continue in 2009. "Bot-nets" technology is used on a regular basis since it allows computer criminals to control networks of computers remotely, however in 2009 "bot-nets" will be capable of multitasking by being able to send spam, hosting malware, and launch direct attacks (Cisco, 2008).

Finally, Cisco (2008) views mobile devices, related web-based tools, virtualization, and remote access to enhance productivity as a major threat. Preventing data loss from outside attackers, or negligence around data storage such as laptops will become a challenge for many organizations. Rapid network expansions and the increase of computer dependability make the current networks more permeable to new Web-based threats.

As mentioned above, the 2009 forecast for cybercrime is grim. Sophisticated organized groups have identified the problems of policing cybercrime.

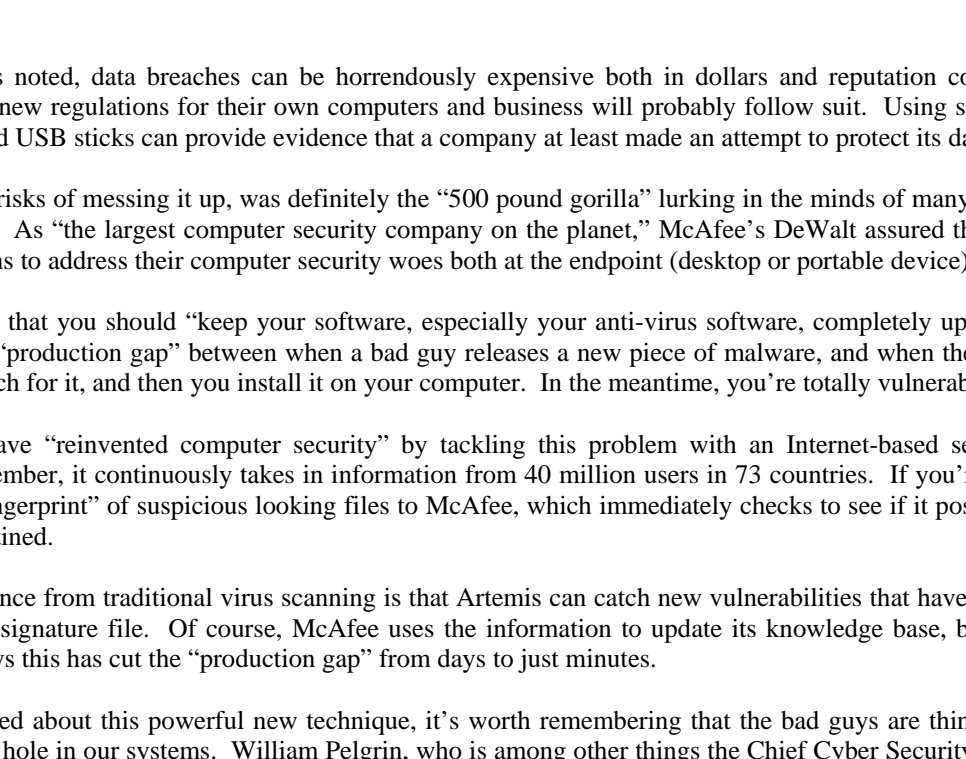
According to Walker and his colleagues (2006), they argue that the traditional policing methods do not apply to cybercrime. In theory, catching a cyber predator is easy, since while using the Internet each user is assigned an Internet protocol (IP) address, which is a unique identifying number on every machine on the Internet.

Every user can obtain an IP address, by subscribing to an Internet Service Provider (ISP). The most common types of ISP are broadband and dial-up. Since millions of people use the Internet, IP addresses have become vulnerable to theft. For example, with wireless routers criminals can obtain an IP address if proper security features are not in place. With the IP address theft, it becomes difficult to track the criminals and time consuming to discover the source of the crime.

The flow chart below depicts how organized crime can commit sophisticated criminal acts without living in British Columbia and without leaving their home.

As a result, this makes cybercrime "one of the fastest growing areas of criminality" (Interpol, 2007-2009).

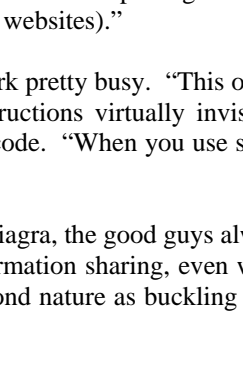
COMPARISONS BETWEEN "REAL-LIFE" CRIME AND "CYBERCRIME"



Websites You Should Visit

- McAfee Threat Center
www.mcafee.com/us/threat_center/default.asp
- Office of the Cyber Security and Critical Infrastructure Centre
www.cscic.state.ny.us
- Federal Trade Commission
www.ftc.gov

If you need to print...

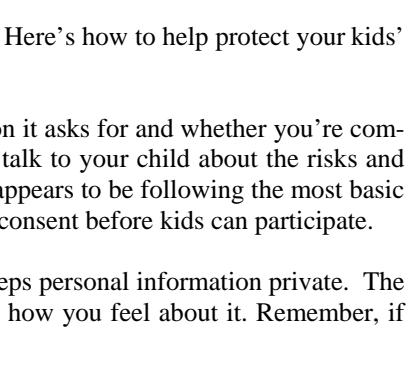


The E-Telligence newsletter is a green document and is not designed to be printed.

If you wish to print an article, just copy and paste the information into a Word document and print in the normal manner. The environment thanks you!

A Report From the McAfee Summit

By Dr. Tom Keenan, Washington, D.C.



Washington, D.C.— Ah, the lone computer hacker, chomping on Doritos in a basement, testing the limits of computer and network security for the sheer joy of knowing. We need to abandon that romantic image, according to Dave DeWalt, the businesslike president and CEO of Santa Clara, California-based computer security firm McAfee Inc. If folks like that still exist, they're now likely to be working for McAfee or a competitor, or, alternatively, in organized gangs trying to steal your money.

"Eighty percent of the malware we're seeing now is financially motivated," DeWalt told an audience of U.S. government security types at the company's recent Public Sector Executive Summit. "As we've watched the economy decline over the past six months, we've seen a complete upward trajectory on the opposite side." He quoted the recent *IBM X-Force Trend and Risk Report*, which, he said, showed a 50 per cent year over year increase in a particularly nasty form of cyber attack – malware on legitimate corporate web sites.

DeWalt dispelled the comforting but erroneous notion that people only get infected if they do something stupid like open an email attachment called I LOVE YOU. "It's just so easy to be able to put malware up on websites," he said, "and then you just search the Internet, click on the website, and you can get infected." In one technical session, a McAfee presenter showed how bad guys can easily trick you into thinking you're on a secure connection at a public access computer, when actually your keystrokes are going to bad guys in the Ukraine.

In fact, you don't even need to get infected. According to a person who should know, some US soldiers in Afghanistan received Amazon "parcel reject" packages in 2008. This can happen when a package is undeliverable and gets returned, supposedly to the sender.

Imagine their glee as they opened the boxes and found shiny new USB thumb drives. Just the thing for storing photos of the family and, well, whatever else soldiers like to keep around. Of course, they poked the USB sticks into the nearest computer. It turns out they were infected with invisible malware, causing a massive problem for the U.S. Department of Defense. Result: in November 2008, the US Army banned the use of removable media. USB sticks are also a common vehicle for corporate espionage and accidental data leakage. DeWalt presented statistics on the number that get left in taxicabs and places like airport lounge computers.

Sensing a market opportunity, security vendors have come up with more secure USB drives, including one that requires biometric activation with the owner's finger. If you knew who to ask (nicely) at this conference, you could get a performance of the SanDisk Cruzer Enterprise FIPS edition. It requires a password and encrypts your data "on the fly" with little impact on performance. The thing is, such devices cost well over \$100 US if you want the secure version. Still, saving a few bucks buying cheapie USB sticks could be a false economy.

As several presenters noted, data breaches can be horrendously expensive both in dollars and reputation cost. Governments are clamping down with new regulations for their own computers and business will probably follow suit. Using something as simple as one of these encrypted USB sticks can provide evidence that a company at least made an attempt to protect its data.

Compliance, and the risks of messing it up, was definitely the "500 pound gorilla" lurking in the minds of many of the government IT honchos in the room. As "the largest computer security company on the planet," McAfee's DeWalt assured them that, for a fee, his company had solutions to address their computer security woes both at the endpoint (desktop or portable device) and the network.

It's become a mantra that you should "keep your software, especially your anti-virus software, completely up to date." But there's still a problem – the "production gap" between when a bad guy releases a new piece of malware, and when the virus companies like McAfee put out a patch for it, and then you install it on your computer. In the meantime, you're totally vulnerable.

McAfee claims to have "reinvented computer security" by tackling this problem with an Internet-based service called Artemis. Announced last September, it continuously takes in information from 40 million users in 73 countries. If you're hooked into it, your computer sends a "fingerprint" of suspicious looking files to McAfee, which immediately checks to see if it poses a threat. If it does, it's deleted or quarantined.

The important difference from traditional virus scanning is that Artemis can catch new vulnerabilities that have not yet been added to your virus checker's signature file. Of course, McAfee uses the information to update its knowledge base, but you get the benefit instantly. DeWalt says this has cut the "production gap" from days to just minutes.

Lest we get too excited about this powerful new technique, it's worth remembering that the bad guys are thinking just as hard, and only have to find one hole in our systems. William Pelgrin, who is among other things the Chief Cyber Security Officer of New York State, made that clear in his talk to the group.

Pelgrin showed how hackers can embed links to their own sites into legitimate websites either to lure people or just to increase their rankings on the search engines so they can sell more Viagra. "We have ability to detect these," he said, "and we're putting out hundreds and hundreds of notices about these to state and local governments around the country (with infected websites)."

Still, the bad guys don't lack creativity and they keep Pelgrin's 24/7 monitoring center in Albany, New York pretty busy. "This one is frightening," he said showing off a technique called "java script obfuscation." It makes the evil instructions virtually invisible. "Some bright, clever person decided that space could equal one and tab equal zero" to replace malicious code. "When you use space and tab what do you get? White space. This one is difficult to very detect."

In chasing the miscreants who want to steal your identity, empty your bank account, or just sell you fake Viagra, the good guys always seem to be playing catch up. Pelgrin says the old method of security is not going to cut it, and that information sharing, even when it's embarrassing, and cooperation are the keys to the future. "Information sharing has to become as second nature as buckling your seat belt."

- www.mcafee.com
- www-935.ibm.com/services/us/iss/xforce/trendreports/
- www.sandisk.com

OnGuardOnline Provides Practical Tips for Parents

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you guard against Internet fraud, secure your computer, and protect your personal information. The Federal Trade Commission (FTC) maintains OnGuardOnline.gov with significant contributions from partners including the US Postal Inspection Service, Department of Homeland Security and WiredSafety.org. One of the topics they recently updated dealt with kid's privacy. One of the many choices kids face online is how to deal with their personal information. Learn more about your rights as a parent and what you can do to help your kids make smart, safe choices online.

What Can You Do?

Your kids' personal information and privacy are valuable — to you, to them, and to marketers. Here's how to help protect your kids' personal information when they're online.

Check out sites your kids visit. If a site requires users to register, see what kind of information it asks for and whether you're comfortable with what they tell you. If the site allows kids to post information about themselves, talk to your child about the risks and benefits of disclosing certain information in a public forum. You also can see whether the site appears to be following the most basic COPPA requirements, like clearly posting its privacy policy for parents and asking for parental consent before kids can participate.

Take a look at the privacy policy. Just because a site has a privacy policy doesn't mean it keeps personal information private. The policy should tell you what the site does with the information it collects; then, you can decide how you feel about it. Remember, if the policy says there are no limits to what it collects or who gets to see it, there are no limits.

Ask questions. If you're not clear on a site's practices or policies, ask about them. If the site falls under COPPA, the privacy policy has to include contact information for the site manager.

Be selective with your permission. In many cases, websites need your okay before they're allowed to collect personal information from your kids. They may ask for your permission in a number of ways, including when by email or postal mail. Or, you may give your consent by allowing them to charge your credit card. In addition to considering when to give your permission, consider how much consent you want to give — in many cases, it's not all or none. You might be able to give the company permission to collect some personal information from your child, but say no to having that information passed along to another marketer.

Know your rights. As a parent, you have the right to have a site delete any personal information it has about your child. Some sites will let you see the information they've collected. But first, they'll need to make sure you really are the parent, either by requiring a signed form or an email with a digital signature, for example, or by verifying a charge made to your credit card. You also have a right to take back your consent and have any information collected from your child deleted.

Report a website. If you think a site has collected or disclosed information from your kids or marketed to them in a way that violates the law, report it to the FTC at ftc.gov/complaint or 1-877-FTC-HELP (382-4357).

Talk, and talk often. Make sure your kids know what information should be private, and what information might be appropriate for sharing. When they give out their personal information, they give up control of who can reach them, whether it's with a marketing message or something more personal. On the other hand, sharing some personal information may allow them to participate in certain activities or to get emails about promotions and events they're interested in.

For more information, visit www.onguardonline.gov

The Future of Internet Warnings for Outages and Viruses

Science Daily (03/16/09) — An early warning system on the Internet could help Europe avoid deliberate or accidental outages, restrict the spread of new viruses, and ensure reliable services, say Malte Hesse and Norbert Pohlmann from the Institute for Internet Security at the University of Applied Sciences in Gelsenkirchen, Germany.

The researchers say there is a growing need to improve the reliability and trustworthiness of the Internet and that raising awareness of critical processes and components on the Internet is essential, particularly among those responsible for the Internet's continued operation. The

Internet's greatest asset is its decentralized structure, but that asset also creates a problem in that it consists of almost 30,000 autonomous systems, each managed by individual organizations primarily within the private sector and there is no governing body for the network. Unfortunately, the private organizations are exposed to a high level of competition, which eliminates the possibility of sharing important management information. If an early warning system is to be built and implemented, a change in attitude is needed. "The cooperation of companies, organizations, and governments is important to create a global view of the Internet," the researchers say. [Click here](#)

The Global Centre for Securing Cyberspace provides a collaborative environment that will directly impact present and future criminality on the Internet. It's a cooperative centre concept dedicated to preventing, reducing and eliminating the criminal advantage of cyberspace. Bookmark www.gcsc.org for our website.

Please email us if you have questions, special events, story ideas or experiences you would like to share. We hope you've enjoyed reading this webletter and we look forward to bringing you E-Telligence again soon.

If you wish to unsubscribe, please contact: kathy.macdonald@gcsc.ca