

2009 Event Calendar

March 29-April 1, 2009
Cambridge University Internet Intelligence Conference
 Cambridge, UK
[Click here](#)

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](#)

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 10, 2009

What's New on the Frontline!

Thought-Leaders Confront Global e-Crime Issues

Peter Cassidy, Secretary General, APWG

CAMBRIDGE, Mass. and LOS ALTOS, Calif. — Electronic crime responders, investigators and counter-electronic crime technologists will join law enforcement and public policy officials from across the globe for the APWG's Counter-eCrime Operations Summit, uniting thought-leaders worldwide to plan the next stage in the global confrontation against electronic crime.

The third annual APWG operations conference (CeCOS III), to be held on May 12-14 in Barcelona, Spain, will engage questions of the conference and the development of common responses for the first responders and forensic professionals who protect consumers and enterprises from electronic crime threats every day.

CeCOS III will present: informative case studies by electronic crime responders and security specialists; examinations of technologies developed and used by electronic crime gangs to exploit Internet infrastructure and user's PCs and client devices; discussions about the technologies and techniques of educating and protecting consumers; and presentations about the development of shared resources like common data formats for e-crime reporting, alerting and coordinating mechanisms.

APWG chairman, David Jevans, says, "National governments, international treaty organizations, law enforcement agencies and industry associations the world over are looking at coordinating data exchange for electronic crime. CeCOS III will work to build bridges between these constituencies that engage the threats that electronic crime poses against consumers and enterprises everywhere everyday."

CeCOS III is an open conference for members of the electronic-crime fighting community, hosted by the APWG and sponsored by LaCaixa, Telefonica, S21sec, GMV, MarkMonitor, EMC's RSA security division, Deloitte España and Ecija. Although sponsorship is principally from industry, the CeCOS programs are considered the most vital events to investigators and managers of electronic crime from across private and public sectors.

In Tokyo last year, at CeCOS II, some 250 delegates attended from law enforcement agencies, technology companies, financial services firms, security services firms, government agencies, consumer advocacy groups and research centers around the globe, bringing together some of the most advanced counter-electronic crime thought leaders from East Asia, Europe, South America and North America.

Parties interested in proposing presentations or participating in panel discussion for CeCOS III can email proposals@antiphishing.org. Parties interested in sponsoring some part of the event can contact Deputy-Secretary General Foy Shiver at fshiver@antiphishing.org. A preliminary working agenda can be found at http://www.antiphishing.org/events/2009_opSummit.html#agenda. The links for registration for this conference can be found at <http://secure.lenos.com/lenos/antiphishing/opSummit09/>.

Welcome to E-Telligence

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

Cyber Warfare: A New Age Battlefield

By Ian Wilms

"On your worst day, you want to be able to make sure that the military [cyber] network still works so that you can effect either the defense of the United States or an offensive action, should they be required... The hardest thing we're going to have to do is to be able to operate this network in time of war. We will be attacked."

— General Kevin Chilton, Commander, Strategic Command, USAF

As I looked around the room, I was pleased to see a packed house and a high number of senior military officials from the United States, Britain, Switzerland, Germany, Belgium, and Israel. Their attendance certainly signified a growing awareness, if not unease, among the global military community of a mounting threat in cyberspace. Unfortunately, as almost every presenter commented, the majority of their political masters still did not have an understanding of the gravity of the threat.

For centuries, nations and states have focused their military strategy around two core pillars — the army and/or the navy. In most countries, the last arm of the military to be created was the air force, roughly at the beginning of the 1920s.

The need to develop another arm of the military, dedicated solely to airpower, grew out of the realization that control of the skies with airplanes would bring a tremendous advantage over the enemy in wartime. It would allow a country to attack quickly over great distances and easily monitor an enemy's movements from a perspective never seen before. Yet at the time, the introduction of the air force to the battlefield, was met with great skepticism. Today, command of the skies has become just as important as dominance on land and on sea.

Is the same skepticism occurring with cyber warfare? Cyber warfare offers the same advantages to those who wish to detect, deter, deceive, disrupt, defend, deny and defeat other nations. A leading panel of experts agreed and discussed at length the best technical ways to improve upon the defence of government and military networks. However, finding an acceptable definition for cyber warfare is causing a huge problem in understanding and responding to incidents of cyber attacks.

There is great hesitancy in the global community to define exactly what cyber warfare is. This appears to be for the simple reason that, if it is defined, then a response must also be prepared and commenced at the right time. Yet, finding a definition of cyber warfare is simple. One just has to look in the U.S. Army Cyber Operations and Cyber Terrorism Handbook 1.02 where the definition states, "cyber warfare and terrorism — the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."

Having the respective global community agree on this definition is one challenge, but building the legal policy and rules of engagement are proving to be an even larger challenge. When one considers that 85 per cent of a nation's critical infrastructure is owned by the private sector, the responsibility for defending it enters a very, very grey area.

The United Nations charter clearly states, "all members shall refrain ... from the threat or use of force against the territorial integrity or political independence of any state, ..." (article 2 (4)). It has been well-documented by experts that they believe it will be only a matter of time before a cyber war breaks out. And some will argue that one has already occurred. NATO did NOT declare the denial of service attacks in Estonia in 2007 to be an "armed attack" but this event certainly fit within the parameters of the definition and, more importantly, caught the world's attention. In the meantime, what needs to be done to prepare for a possible cyber war?

An idea that was debated at the conference involved developing a deterrence policy for cyber weapons. After all, to successfully deter an attack, one first needs the capability to trace the origin of the attack. This can only be accomplished through the active capability to actually trace back the attack. All of which ultimately requires collaboration among industry, academia, law enforcement, and the intelligence community. From this collaboration, cyber weapons can be developed and potentially used to suppress the use of enemy cyber weapons.

To properly tackle the problem, one presentation recommended that governments everywhere begin updating military policies to define what an act of cyber war is, and what the response should be. If a nation's cyber infrastructure were to be attacked or knocked offline today, which organizational structure would take the lead to quickly get operations back online? The priority must be for a country to determine which group would have the overall leadership responsibility to get things back up and running.

Other nations are now recognizing the importance of securing cyberspace. In the United States, President Obama has stated that he will "make cyber security the top priority that it should be in the 21st century..." He recently stated, "I'll declare our cyber infrastructure a strategic asset and appoint a national cyber advisor who will report directly to me. We'll coordinate efforts across the federal government, implement a truly national cyber security policy and tighten standards to secure information — from the networks that power the federal government to the networks that you use in your personal lives." What will it take to convince our respective political leaders to take a similar proactive approach?

The overall theme heard at the conference was exercise, exercise and more exercise. It is only through constant training that weaknesses will be exposed and patched. While cyber warriors may not be regarded as "real" soldiers by some, make no mistake that these cyber warriors will be making a critical contribution to future battles in both the physical and cyber world. The cyber warfare powers of the future will not be judged on how many computer warriors they have in demographics but rather on how intelligent the soldier is behind the keyboard and how advanced, the technology is they are using.

Ian Wilms, is the chair of the Global Centre for Securing Cyberspace and is the past president of the Canadian Association of Police Boards. He recently attended the Cyber Warfare 2009 conference in London, England.

Websites you should visit...

Multi-Function Criminal Justice Support
<http://criminaljustice.state.ny.us>

New Portal for Community Interaction
<http://citizenship.microsoft.ca>

New Zealand Educational Non-Profit Organization
<http://www.netsafe.org.nz>

Citizenship Portal Now Live



By Gavin Thompson, Director of Citizenship, Microsoft Canada

I'm fortunate to have two roles I love — one is being a father and the other is leading our citizenship initiatives for Microsoft in Canada. In both roles, I am equally passionate about keeping children safe and secure, especially online.

That's why I'm pleased to share some new research that we did examining the ever-changing online habits of Canada's youth. Online safety has become a top priority for parents, law enforcement, educators and young people. We wanted to know what has been resonating with youth and what we should be concerned about when our kids are online.

So last month we teamed up with Youthography, a market research firm that deals specifically with young people and questioned more than 1,000 Canadians aged 9 to 17 to better understand their online activities.

The results show that the Internet is an overwhelmingly positive force in the lives of Canadian youth. Most are aware of potential dangers and parental engagement in cyberspace is high.

However, too many children and teens still engage in risky behaviour while online. Specifically, by sharing too much personal information on social networking sites, communicating with strangers, cyberbullying and actively seeking out adult content.

One of Microsoft's highest priorities is protecting children online and ensuring they have a safe and enjoyable experience. For several years we have engaged in public education awareness campaigns, worked with law enforcement agencies and conducted research into online behaviours.

We will use the information in this survey to work with national organizations and youth to develop a comprehensive campaign to educate Canadians about risky online activities.

For more information on our online safety initiatives please visit our citizenship portal — a place to get information and hear stories about Microsoft's commitment to this great country.

We created this portal for one simple reason — in talking with many of you, we know that you are committed to making a positive difference in Canadian communities. The more we share our experiences with each other, the greater impact we can all have.

We've designed this portal to be interactive, so please, take a look around and share your comments and stories with us at <http://citizenship.microsoft.ca/>.

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!

You'll be Interested in This

Hackers Still Enjoy Vandalizing Web Sites IDG News Service (02/26/09) ; Kirk, Jeremy

A small study of Web site hacks reveals that 24 percent of hackers participate in ideological hacks, or site defacements that do not involve money or data theft. The findings of the recent Web Hacking Incidents Database Annual Report indicate that financial gain is not always the primary purpose behind vandalism, though most hacks in recent years have been predatory in nature, according to the study, sponsored by the security products firm Breach Security and the Web Application Security Consortium. Researchers set a list of criteria for site hacks they wanted to study. All were publicly reported, had correlating web security issues, and had a tangible effect on a business. The report, which examined 57 out of hundreds of thousands of site hacks that occurred in 2008, found most acts of vandalism "were of a political nature, targeting political parties, candidates and government departments, often with a very specific message related to a campaign. Others have a cultural aspect, mainly Islamic hackers defacing western web sites." Nineteen percent of the defacements were accompanied by data theft, 16 percent malware, and 13 percent organizational damage. ([go to web site](#))

APWG Publishes Anti-Phishing Advisory on Troubling Abuse of Subdomains Business Wire (02/26/09)

A new report from the APWG, an independent coalition that is working to fight cybercrime, shows that more than 10 percent of all phishing sites originate on subdomains that are available for registration at subdomain registry services. The report noted that cybercriminals use these subdomains for their phishing sites because their low- or no-cost pricing models, anonymity, easy set-up, and lack of internal organization, dispute rules, or policing make them easy to exploit. Rod Rasmussen, one of the authors of the report, notes that cybercriminals particularly like to exploit subdomains of free Web hosting companies since these domains are so difficult to shut down. The report also says that cybercriminals are always looking for other ways to distribute phishing emails and lure web surfers to malicious sites. In addition, the report finds that cybercriminals often take a number of steps to protect their scams from being detected by law enforcement agencies and Internet service providers. ([go to web site](#))

GCSC to Host eBay Law Enforcement and Private Security Training Session

CALGARY, Alta. and SAN JOSE, Calif. — GCSC is very pleased to announce that on April 9, 2009, it has invited officials from eBay Inc. and PayPal to an informational training session for law enforcement and private security officers. This session will provide a better understanding of how the eBay and PayPal platforms work and will inform attendees how eBay and PayPal assist with investigations. This half-day session will be held at no-charge at a location in Calgary to be announced very soon.

Law enforcement and retail loss prevention departments often seek assistance with their investigations relating to eBay and/or PayPal. This session will answer those questions and will also offer an understanding of the eBay's and PayPal's global resources that help law enforcement and private security do their job. eBay strongly believes in working closely with the police, private and corporate security investigators and other government agencies to help keep our community safe. Their safety teams include former law enforcement officials from around the world and we are very pleased to have Jack Christin, senior regulatory council on eBay and Mike Rou, senior manager of investigations from PayPal at this session.

There is limited space available and the session is open to any law enforcement and private security officers on a first come, first serve basis. To attend please contact Kathy at kathy.macdonald@calgarypolice.ca. This session is supported by ASIS Chapter #162.

What You Need to Know About Video Games and Children

Ten Tips for Parents

- CHECK game rating and read the description. Rent a game to preview before purchasing. Some major online games have ESRB ratings; others do not. Check out online reviews.
- AVOID the "first person shooter," killographic games. Instead, pick non-lethal games that require the player to come up with strategies and make decisions in a game environment that is more complex than punch, run, and kill.
- LIMIT game playing time. (Recommendation: no more than one hour per day)
- WATCH for warning signs of video game addiction. Stop obsessive playing before it gets out of control. Encourage your child to play with friends "off line" away from the computer.
- TALK with your children about griefers and cyberbullying. Establish house rules of "netiquette" and follow through with consequences if rules are broken. Encourage your children to talk to you if they see inappropriate behavior online.
- DISCUSS the content of games and explain why you object to certain games. Remember that children also play video and computer games outside of the home. What are the gaming rules at their friends' homes?
- SET clear house rules around Internet and game use and time. Require that homework and chores be done before playing.
- DO NOT PUT video games or computers in kids' bedrooms. Place video game consoles and computers where it is easy to monitor.
- MEETING online gaming requires adult supervision. Your kids may feel quite close to other gamers they meet online. Remind them that these people are still strangers and that it isn't safe to meet them alone.
- DON'T assume that other parents' judgments on video games will be the same as yours. You may agree on some things, but may not on this subject.

— Source: Department of Criminal Justice Services New York State

The Global Centre for Securing Cyberspace provides a collaborative environment that will directly impact present and future criminality on the Internet. It's a cooperator 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