

THE CPIIRC NEWS



The Canadian Private Investigators' Resource Centre Welcomes Our Newest International Members

Inside this issue:

Welcome To Our Newest International Members	1
Canadian Terror and Intelligence News Wire	2
Homemade GPS Jammers Raise Concerns	3
Computer Quick Tips	4
Proper Techniques for Witnessing A Confession	5-8
Resource Centre Roundup	9
Contact Information	10

AFRICA

Cameroon 
Worldwide Investigators Agency

Nigeria 
THEOSEARCH INTERNATIONAL LTD

EUROPE

Belgium 
de Kort & Partners Ltd.

Greece 
KSA Security

Ireland 
Priority Investigations

The Netherlands 
International Security Partners

Portugal 
W.I.S International

Switzerland 
Business Control (Switzerland) Ltd.

ASIA


India 
Lancers Network Limited

India 
Premier Shield Pvt Ltd


Malaysia 
SJ Security Consultants

Pakistan 
Risk Identifications Private Limited


Philippines 
Orion Support Incorporated (OSI)


United Arab Emirates 
Premier Shield Security Services


NORTH AMERICA


Cayman Islands 
Intelsec Consultants Limited

Mexico 
AM-MX Investigations

United States of America 
Beacon Investigations, LLC

United States of America 
DCRI, LLC. Private Investigations

United States of America 
Northshore Process Service

United States of America 
Spectre Inc.

Canadian Terror and Intelligence News Wire



Canada's Oil Industry A Possible Al Qaeda Target

Updated Wed. Oct. 10 2007 1:47 PM ET

The Canadian Press

MONTREAL – A Canadian Security Intelligence Service document obtained by a Quebec newspaper says terrorists have included Canada's petroleum industry among their possible targets.

The potential Al Qaeda targets were included in a risk-assessment document prepared for CSIS and obtained by Montreal's Le Devoir under the Access to Information Act.

The newspaper reports today that North America's electricity network is also a potential target.

The document says petroleum industries in Mexico and Venezuela were also proposed as targets by a publication sympathetic to al Qaeda on February 9.

Era of espionage not over, CSIS says

Spies now focus on labs and boardrooms, not military HQs.

By CP

OTTAWA – The Cold War is long over, but foreign spies are still trying to infiltrate key federal departments in a continuing quest for secrets, says Canada's intelligence agency.

In its latest annual report, the Canadian Security Intelligence Service warns scientific and technological developments in Canada's natural resource sector are also a prime target.

CSIS used the report, tabled in Parliament yesterday, to remind Canadians that the threat of espionage remains worrisome even though terrorism has become the main concern of the modern era.

Increasing global competition is prompting foreign spies to shift their focus away from the political and military secrets of the past and toward illicit acquisition of economic and technological information, the report says.

While CSIS singles out no country by name in the report, the service says both "traditionally hostile and ostensibly friendly" governments have engaged in spying against Canada.

Guansheng Han, a security official who defected from China, told CP last year that Beijing cultivates sources in the Canadian Chinese community as a way of gleaning intelligence on key economic sectors, including the bio-pharmaceutical industry.

China has denied spying on other countries.

According to CSIS, Canada has been targeted by nations seeking advantages in fields such as aerospace, biotechnology, chemicals, communications, information technology, mining, metallurgy, nuclear energy, oil, gas and environmental technologies.

Homemade GPS Jammers Raise Concerns

Government officials and communications experts are assessing the public safety and security implications of a newly posted online article that provides directions for making cheap devices that can jam Global Positioning System (GPS) signals.

Information in the article that appears in the current issue of the online hacker magazine Phrack potentially puts at risk GPS devices used for commercial navigation and military operations, authorities said. The Phrack article provides a detailed guide to building a low-cost, portable GPS jammer out of components that can be easily obtained from electronics supply houses. According to the article, the "onslaught of cheap GPS-based navigation (or hidden tracking devices) has made it necessary for the average citizen to take up the fine art of electronic warfare." Electronics and GPS experts who read the article this week called it technically competent and said amateurs with a certain amount of technical skill could build a GPS jammer from the plans.

Although the article said the jammer is designed to work only against civil-use GPS signals broadcast on the frequency of 1575.42 MHz and not the military frequency of 1227.6 MHz, James Hasik, an Atlanta-based consultant and author of the book *The Precision Revolution: GPS and the Future of Aerial Warfare*, disagreed. Hasik said that while the Phrack jammer is targeted at civil GPS signals, known as the C/A code, it could also threaten military systems, since "almost all military GPS receivers must first acquire the C/A signal" before locking onto the military signal, known as the P(Y) code. Hasik said that GPS receivers are especially vulnerable to jamming because of low signal strength after traveling through space from GPS satellites orbiting 12,000 miles above the earth. The U.S. Department of Defense, which faces the possibility of having its GPS-guided weapons come up against Russian-made GPS jammers in Iraq, has anti-jamming technology at its disposal. Still, Defense officials viewed the Phrack article with concern.

Air Force Lt. Col. Ken. McClellan, a Pentagon spokesman, said the implications of homemade jammers described in the article are "somewhat serious" because the use of such jammers "could disrupt commercial operations." McClellan said GPS experts at the Pentagon do not "at the moment" view homemade jammers as a hazard to flight safety for commercial aircraft or ship operations, "but rather a nuisance." The Federal Aviation Administration is developing a nationwide GPS-based precision landing system. And the Coast Guard operates a GPS-based maritime navigation system on both coasts, the Great Lakes, inland waterways and Hawaii. Bill Mosley, a spokesman for the Department of Transportation, the parent agency of the FAA and the Coast Guard, said his department is well aware of the threat posed by GPS jammers.

This article was reproduced from a January 17, 2003 Computer World article.

How much private information can you collect from a website?

When you register a domain, you must give valid contact information. It goes into the WHOIS database. This poses a big risk: This database is available to anyone online and it only takes seconds to find your address and phone number.

To protect your personal information from being viewed by anyone who has access to the internet Network Solutions has a feature called Private Registration. They will provide alternate contact information for the listing of your domain name registration(s) in the public WHOIS database. Not only will this protect your personal information but will also control the amount of spam you receive in your inbox. For more information visit www.networksolutions.com

Computer Backups Made Easy

You know that creating regular backups of your computer files is important, but you never seem to get around to burning those CDs or copying your files to your external hard drive?

PC Backups with Carbonite automatically finds all your data files – documents, photos, music, emails, first encrypts them and then backs them up over the internet to Carbonite's secure servers for less than \$5/month. For more information visit www.carbonite.com/

Free Text Messaging

Trying to save on your cell phone bills by sending out text messages instead? Unless you have a text message plan most text messages costs around .15 cents per text. Now you can send FREE text (SMS) messages to any cell phone in the U.S. and Canada. You can send 10 free messages per day or sign-up for unlimited access.

Click on the link [Free Texting Messaging](#) found in the “Telephone Directories/Areas Codes/Postal Codes” category in the Resource Centre.

Removing Unwanted Software From Your Computer

Whenever buying a new computer they often come loaded with trial software that most people never use taking up valuable hard drive space and can even slow down your system. The “PC Decrapifier” is a free software that detects the most common unwanted softwares and gives you the option to uninstall the least desired ones.

Click on the link [PC Decrapifier](#) found in the “Free Investigative Software & Publication Downloads” category in the Resource Centre.

SUN TZU

The author of The Art of War, an immensely influential ancient Chinese book on military strategy.

The works of Sun Tzu has been applied to business, sports, diplomacy, personal lives and has been popularized in business and management texts. Sun Tzu may be the most frequently quoted Chinese personality in the world today. Some of his more known quotes;

“All war is based on deception. “

“He who knows when he can fight and when he cannot, will be victorious.”

“You have to believe in yourself.”



Circa 500 BC

Proper Techniques for Witnessing A Confession

No investigator wants to have his testimony questioned because it is his word against the defendant's. It is precisely for this reason that the investigator needs to have a witness verify that the investigator's testimony is accurate. While it sounds like a simple concept, there are important considerations and procedures to follow when having a confession witnessed.

This point became evident in the recent case of Commonwealth v. Miller. In this case, an Appeals court ruled that the trial judge committed reversible error for not holding a hearing to examine the voluntariness of a confession obtained by loss prevention investigators employed by the defendant's ex-employer. At issue were extremely discrepant accounts of an in-house interrogation of an employee suspected of stealing \$1,000.

The two investigators described a "low-key inquiry" of the defendant. They testified that the defendant "vented" during the two hour interrogation, but ultimately broke down and confessed to stealing the missing \$1,000. The investigators denied doing or saying anything to threaten the defendant and testified that the defendant did not exhibit any physical manifestations of being threatened or intimidated.

Conversely, the defendant testified that she felt afraid as she was escorted to an unfamiliar room and questioned by two strangers. She described the room as small and said that she felt claustrophobic. According to the defendant, one investigator "loomed over her and made threatening gestures" while the other blocked the door. The defendant claimed that she was denied a request to call her husband or an attorney. She further claimed that the investigators suggested that if she did not confess that the case would be turned over to the police which may result in a conviction which, in turn, could lead to the defendant's separation from her special needs child.

As to the confession itself, the defendant testified that throughout the writing, editing and signing of the confession she protested her innocence. According to the defendant, the message conveyed to her was that she would not be allowed to leave the room until the papers were signed. At trial, the defendant's husband testified that his wife was crying and sounded distressed during a phone call to him following the interrogation. This was corroborated by a witness who heard the husband's side of the phone conversation. A point not contested was that the investigators violated company policy by failing to have a supervisor present during the interview and interrogation of the employee.

Long before devices were available to electronically record interviews and interrogations, investigators utilized a witness to document what happened during an interview or interrogation and to verify that the suspect, in fact, did offer a voluntary and trustworthy confession. The Miller case serves as an important reminder that if an interview or interrogation is not electronically recorded, it is imperative that the investigator follow proper procedures when having a confession witnessed.

It will be helpful to introduce this topic with a fundamental review of the psychology of deception. Everyone lies for exactly the same reason; all lies are motivated to avoid the consequences of telling the truth. The consequences a deceptive suspect fears may involve loss of income or freedom (being fired, going to jail) as well as loss of pride or self-worth (having to face co-workers or a spouse). Consequently, during an interview or interrogation the investigator wants to do everything legally possible to reduce perceived consequences of telling the truth. One of the most important considerations in this regard is to conduct interviews and interrogations in private.

Privacy is considered the single most important psychological factor contributing to the success of an interview or interrogation. Very simply, it is easier for someone to reveal sensitive information to one person than to two people. Furthermore, it is easier to reveal sensitive information to someone who is not associated with consequences than to a person who represents consequences. Would a child rather confess wrong-doing to a parent or a kindly uncle?

In our text books and other web tips we have offered many examples illustrating the importance of privacy. The following experience comes from a recent seminar participant. For many years he conducted loss prevention interviews and interrogations in private, working one on one with employees. He enjoyed great success learning the truth in a private environment and having the employee's confession witnessed by a supervisor following the interrogation.. This year his employer required that the employee's supervisor be present during the entire interview and interrogation. The investigator reported that he rarely obtains a confession with the supervisor present during the interrogation.

Because of the importance of privacy, an investigator should do everything possible to conduct interviews and interrogations in such a way that the suspect is only communicating with a single investigator. However, it is also important to have a witness to this procedure. There are two procedures commonly utilized to document a suspect's confession and the events that led up to it. The first is to have a witness present during the entire interview and interrogation process. Second, the investigator can bring someone into the room to witness the confession after it has been obtained. Under most circumstances, it is to the investigator's advantage not to have a witness present during the entire interview and interrogation. An exception is when there is an obvious liability risk such as when a male investigator interviews a female subject concerning a sexual issue.

If a witness is present during the entire interview and interrogation that person should be someone who is not socially acquainted with the suspect e.g., another investigator, manager from a different department, clerical staff. Furthermore, the witness should sit out of the suspect's sight and remain silent throughout the interview and interrogation. Certainly, the witness should not be involved in questioning the suspect, i.e., the witness is merely an out-of-sight, uninvolved, observer.

In the Miller case the "witness" was an investigator actively involved in trying to get the defendant to confess. The court recognized that this "witness" was motivated to deny that any wrong-doing occurred during the interrogation. A person involved in obtaining incriminating information can hardly be considered an objective, impartial witness to the confession.

If two investigators are present during an interview or interrogation, it is our recommendation that they not "team up" on the suspect where both investigators simultaneously ask questions or make persuasive statements. Rather, one investigator should be the communicator and the other should be an observer. The communicator should be seated directly in front of the suspect and do all of the talking. The observer should be out the suspect's sight and remain silent. It is acceptable for the investigators to switch roles, where the observer becomes the communicator and vice versa. In doing so, however, the investigators should also switch chairs so the new observer is out of the suspect's sight. For obvious reasons, if two investigators are involved in obtaining a confession, the witness to the confession should be a third person brought into the room for that purpose following the interrogation.

If the decision is made to not have the witness present during the entire interview and interrogation, the witness would come into the room following the suspect's confession. It is important that this witness can testify not only that the suspect offered a trustworthy confession, but also that the confession was voluntary. It was the absence of such testimony that greatly contributed to the reversal in the Miller case.

The witness who comes into the room following the confession may be another investigator, the suspect's supervisor or a manager from a different department. The conversation with the suspect, Randy, would be similar to the following, "Randy, this is Mr. Buckley, my boss. I just want to let him know what you've told me this afternoon." At this point the investigator and witness would face each other and the investigator would repeat the suspect's confession in the presence of the suspect and the witness, e.g., "Randy told me that he is the person who stole \$1,000 from his cash drawer last Friday afternoon. He said that he stole the money at the end of the day at around 5:15, when he was balancing out his drawer. He needed the money because of ..." It is important that while the investigator repeats the suspect's confession, that the investigator and witness continue to look at each other and not look down at the suspect.

It is improper, and psychologically wrong, to ask the suspect to repeat his confession in the presence of the witness. Under this circumstance, the suspect is unlikely to offer a fully detailed and corroborated confession in the presence of a stranger. However, once the suspect knows that the witness has heard the truth, most suspects will openly discuss their crime. At this stage of the process it is important that the witness independently question the suspect about his crime. The questions the witness asks should develop information to corroborate the suspect's confession. In addition, because the witness was not present during the entire interview and interrogation, it is important that the witness ask the suspect questions to develop information to demonstrate that the confession was obtained without threats or promises. The following questions would each help accomplish these goals:

"Is everything Mr. Jayne said accurate?"

"Do you have any of the money left?"

"Have you stolen money from the company before this?"

"What bills did you pay with the money you stole?"

"Do you have any complaints about the way Mr. Jayne treated you?"

"Were you threatened in any way today?"

"Did anyone offer you any promises?"

The witness to a confession should be able to testify not only about the suspect's physical appearance and emotional state following the confession, but also that the suspect's confession was trustworthy and was the product of the suspect's free will.

A very troubling aspect of the Miller case is that the defendant claimed that she was protesting her innocence throughout the process of developing the written confession. It is one thing for a defendant to recant a confession at some point after making it – that is not unusual. However, to have a subject state that she was denying committing the crime at the time the confession was being given, edited and signed represents either an incredibly bald-faced lie under oath or a person who was coerced into signing a confession. Unfortunately, in this case no witness was brought into the room to independently assess the suspect's emotional state, or to elicit information from the suspect about the details of her theft, to find out if she was threatened in any way, had complaints about the way she was treated, etc.

In conclusion, there is no question that the best technique to document the events of an interview or interrogation is a surreptitious electronic recording. When this option is not available, the investigator should have a suspect's statements witnessed by a person not involved in obtaining the confession. If the witness is present during the entire interview and interrogation, the individual should not be someone personally acquainted with the suspect. Furthermore, that person should sit out of the suspect's sight. If a witness is brought into the room following the confession, the investigator should repeat the suspect's confession in the presence of the witness who should then independently question the suspect to obtain corroboration that the suspect, in fact, committed the crime and to elicit information to assess the voluntariness of the confession.

The topic covered in this web tip is derived from information covered during our advanced course on interviewing and interrogation. If you have attended our basic course and are ready to enhance your ability to detect deception and elicit confessions, check our course calendar for the location of the advanced course nearest to you.

For further information on interrogation or interviewing techniques consider attending our advanced course on interviewing and interrogation. All CPIRC members get discounts on Reid seminars.

This article was prepared by John E. Reid and Associates, Inc. as their Monthly Web Tip and was reprinted on our web site with their permission. For additional Monthly Web Tips, go to www.reid.com and click on "Helpful Info".

Resource Centre Roundup

ICHAT The Internet Criminal History Access Tool

The Internet Criminal History Access Tool (ICHAT) allows the search of public records contained in the Michigan Criminal History Record maintained by the Michigan State Police, Criminal Justice Information Center. All felonies and serious misdemeanors that are punishable by over 93 days are required to be reported to the state repository by law enforcement agencies, prosecutors, and courts in all 83 Michigan counties.

Click on the [ICHAT](#) link found in the "Resource U.S.A" category in the Resource Centre.

U.S. News Archives On The Web

Quickly search U.S. news archives available on the Web.

- Sources are arranged by state.
- Unless noted, searching is free.
- If you don't find what you're looking for, other sources are available.
- Archives of international, Canadian, as well as Asian news sources are also available.

Click on the [U.S. News Archives On The Web](#) link found in the "Resource U.S.A" category in the Resource Centre

U.S. Securities and Exchange Commission

The mission of the U.S. Securities and Exchange Commission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.

All companies, foreign and domestic, are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Anyone can access and download this information for free. Here you'll find links to a complete list of filings available through EDGAR and instructions for searching the EDGAR database.

Click on the [U.S. Securities and Exchange Commission](#) link found in the "Resource U.S.A" category in the Resource Centre

SITE INSTITUTE

The Search for International Terrorist Entities

"By monitoring terrorist and extremist websites and penetrating password-protected Al Qaeda linked sites, SITE provides a state-of-the-art intelligence service to both practitioners and analysts to understand the adversary." - Rohan Gunaratna, Author, Inside Al Qaeda: Global Network of Terror (Columbia University Press).

Studying the primary source propaganda, training manuals, and chatter of terrorists offers insight into terrorists and their activities that can not be obtained anywhere else. Failing to monitor terrorist propaganda is a failure in intelligence. To fulfill this need, the SITE Intelligence Group offers its Monitoring Service, which provides numerous daily translations of terrorist propaganda and multimedia from primary source terrorist websites.

Click on the [SITE Institute](#) link found in the "Security and Intelligence Community" category in the Resource Centre.

HOW TO CONTACT US



Monday to Friday	09:00 -17:00 (Eastern Standard Time)
Saturday & Sunday	Via Email Only
Canadian Statutory Holidays	Closed

Telephone:	(514) 373-8191
Fax Inquiries:	(514) 303-8841
Mailing Address:	CPIRC 2348 Chemin Lucerne, Suite #506 Ville Mont-Royal, QC H3R 2J8 Canada

To contact CPIRC via email please [click here](#).

www.cpirc.com

