



## ARCHIVED - Archiving Content

### Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

## ARCHIVÉE - Contenu archivé

### Contenu archivé

L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

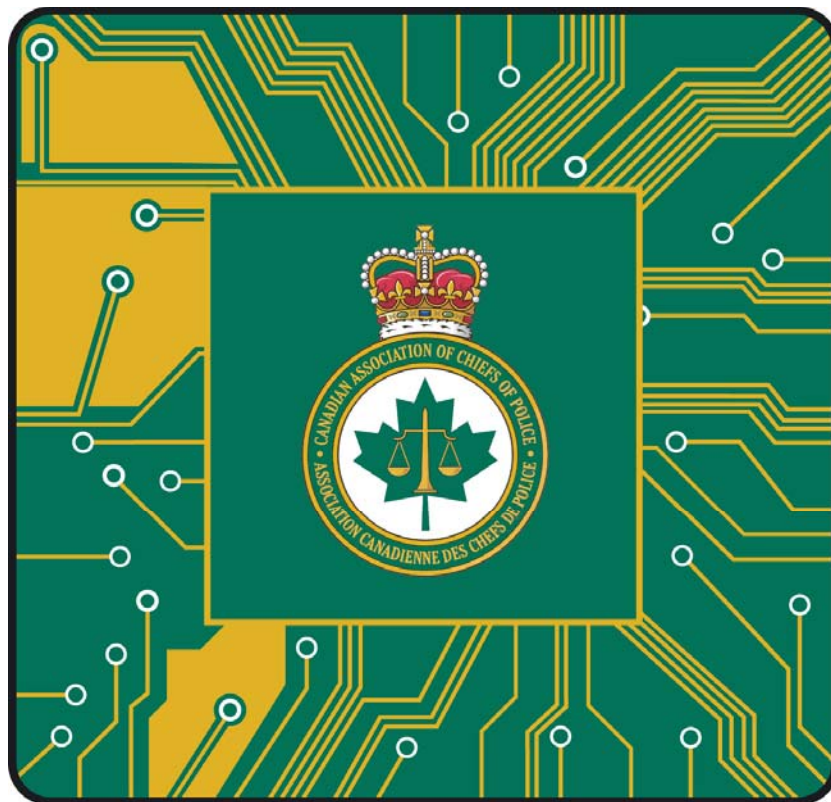
Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.

<p><b>Canadian Association of Chiefs of Police</b> Leading Progressive Change in Policing</p>		<p><b>L'Association canadienne des chefs de police</b> À l'avant-garde du progrès policier</p>
---	---	--

## Electronic Crime Committee 2006 Annual Report



**CACP e-Crime Committee**

## **TABLE OF CONTENTS**

---

Table of Contents.....	2
2006 Message from the Chair.....	3
Committee Mandate/Objective.....	5
Dates/Overview of Meetings.....	6
Summary of Initiatives/Activities 2005/2006:.....	8
Summary of Resolutions.....	10
Resolution on Training in Computer Forensics Commentary.....	10
Resolution for Minimum Sentence for Luring Offences Commentary.....	12
Activities Planned/Significant Dates.....	15
Committee Members List:.....	16
CHAIRPERSON.....	16
Ken C. Smith.....	16
MEMBERS.....	17
Ray Archer.....	17
Richard C. (Dick ) Bent.....	18
Alain Dubuc.....	19
Steve Izzett.....	19
David Korol.....	20
Réal Laguë.....	21
Bessie Pang.....	21
Tom Pownall, MBA.....	22
Paul L. Roy.....	23
Associate Corporate Member.....	24
Michael Kert Eisen.....	24
Technical Advisors.....	25
Susheel Gupta.....	25
Dan MacRury.....	25
Gareth Sansom.....	26
Alex Smith.....	27
Arni Stinnissen.....	27
France Thibodeau.....	28
Appendix “A”.....	29
Appendix “B”.....	35
Appendix “C”.....	43

## **2006 MESSAGE FROM THE CHAIR**

We are pleased to report on the activities of the e-Crime Committee.

The e-Crime Committee continued to follow the Strategic plan developed and introduced in 2004. The strategic plan provides a road map to ensure that our committee activities are aligned with our strategic mission as well as the goals and objectives of the CACP. Our Committee will be action oriented to achieve the ultimate outcomes of our strategic plan. We remain committed to working closely with other committees of the CACP.

In 2005 Co-Chair Superintendent Doug Lang, RCMP stepped down from the Committee to pursue other operational demands. On behalf of the e-Crime Committee I would like to thank Doug for his leadership and dedication to the importance of electronic crime as we move into the 21<sup>st</sup> century.

We have made efforts to establish membership that is truly national and reflects Canadian police leaders, private sector members, and prosecutorial experts. To that end we have extended our outreach to include membership representation from the Province of Quebec. In fact, Inspector Réal Laguë of the Sûreté du Québec hosted one of our Committee meetings in Montreal and involved participation from the Montreal Urban Police. Superintendent David Korol of the Edmonton City Police hosted the spring meeting.

In 2005 the Committee welcomed membership from Inspector Steve Izzett, Toronto Police Service and Inspector Paul Roy from the Ottawa Police Service. We also welcomed Ms. France Thibodeau from the Canadian Police College to further our commitment to exploring effective training strategies in both official languages for e-Crime investigators.

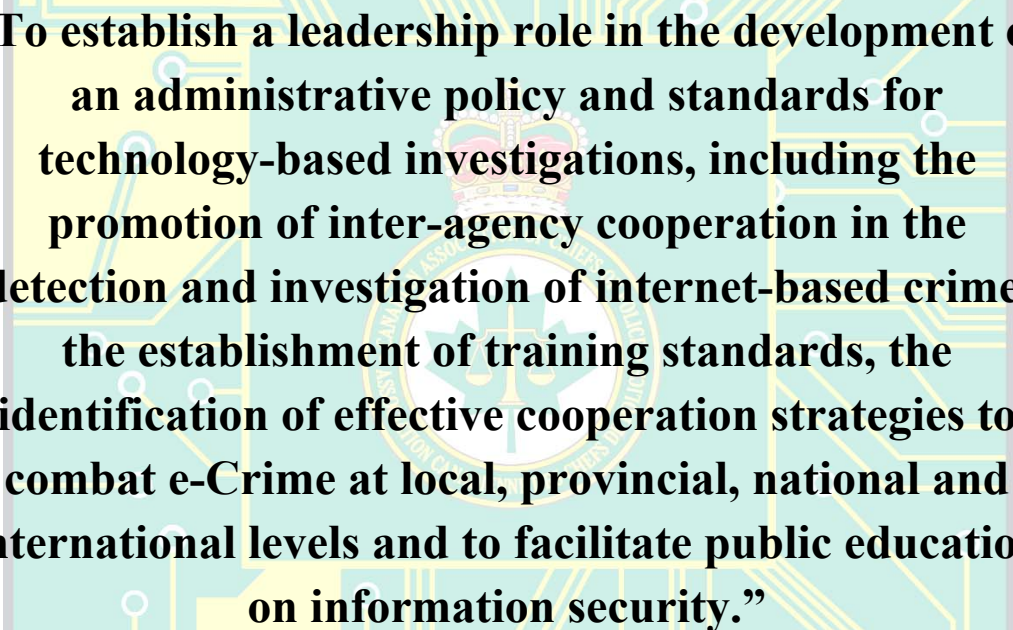
Canada's police services must meet the challenge to stay ahead of Electronic Crime challenges. This Committee continues to be the best avenue for all Canadian police services, federal, provincial and municipal, to share in each others knowledge, skills and abilities, to augment current strategies in combating e-Crime.

In a recent interview with Her Majesty's Inspectorate of Constabulary Chief Constable Dennis O'Connor he noted that one of the biggest challenges facing policing in Britain was the exponentially rising costs associated with combating technological crime. That challenge exists as well for policing in Canada where every fraud, sexual assault, homicide and public security investigation will call upon highly trained e-Crime investigators to respond and support these investigations.

The future is upon us and the safety of our communities requires an effective investment in e-Crime capabilities.

Chief Superintendent Ken C. Smith  
Ontario Provincial Police  
e-Crime Committee Chair

## **COMMITTEE MANDATE / OBJECTIVE**



**“To establish a leadership role in the development of an administrative policy and standards for technology-based investigations, including the promotion of inter-agency cooperation in the detection and investigation of internet-based crime, the establishment of training standards, the identification of effective cooperation strategies to combat e-Crime at local, provincial, national and international levels and to facilitate public education on information security.”**



**CACP e-Crime Committee**

## **DATES/OVERVIEW OF MEETINGS**

The e-Crime Committee meets approximately every 4 months in each calendar year in different parts of Canada. Committee members are currently hosting the meetings and any expenses incurred are borne by the host. CACP Board of directors provides funds to offset these expenses of non-police members to attend as well as expenses of ancillary expenses.

### **August 21, 2005**

The summer/fall 2004 meeting of the e-Crime Committee was held on August 21, 2005 at the Westin Hotel, Ottawa. In attendance were:

Ken SMITH (Co-Chair)	OPP
Doug LANG (Co-Chair)	RCMP
Ray ARCHER	CBA
Dick BENT	RCMP
Mike EISEN	Microsoft
Jim RAMER	Toronto Police
Alex SMITH	Attorney-General Ontario
Arni STINNISSSEN	OPP

Items discussed included First Responders Guide, Correspondence to Canadian Internet Registry Association, Canadian Police College presentation, Discussion on Security of Information Act, CETS update, Linkages to other CACP committees and the e-Crime Strategic Plan. Full Meeting minutes available in this report as Appendix “A”.

### **January 19, 2006**

The Winter 2004/2005 meeting of the e-Crime Committee was held on January 19, 2006 at the Sûreté du Québec HQ in Montreal which had the highest attendance to date. Members participating included:

Ken SMITH (Chair)	OPP
Dick BENT	RCMP
Tom POWNALL	RCMP
Steve IZZET	Toronto Police
Keith WHITTON	Edmonton Police (representing David KOROL)
Mike CALLAGHAN	Ottawa Police (representing Paul ROY)
Réal LAGUË	Sûreté du Québec
Stephen BOUCHARD	Montreal Urban Police
Francesco SECONDI	Montreal Urban Police
Alain DUBUC	Sûreté du Québec

France THIBODEAU  
Gareth SANSOM  
Ray ARCHER  
Arni STINNISSSEN  
Dan MACRURY  
Alex SMITH  
Bessie PANG

Canadian Police College  
Justice Canada  
Canadian Bankers Association  
OPP  
Public Prosecution, Nova Scotia (by phone)  
Attorney-General, Ontario (by phone)  
Society for Policing Cyberspace (by phone)

Items discussed included Resolution proposals, Law Amendments Report, Quebec-wide working group on tech crimes. Minimum training standards, certification, IP address blocking, report from PolCyb. Full Meeting minutes available in this report as Appendix “B”.

### **May 25, 2006**

The Spring/Summer 2006 meeting of the e-Crime Committee was held on May 25, 2006 at the Edmonton Police Headquarters in Edmonton. Members participating included:

Ken SMITH (Chair)	OPP
Dick BENT	RCMP
Paul ROY	Ottawa Police
Tom POWNALL	RCMP
David KOROL	Edmonton Police
Réal LAGUË	Sûreté du Québec
Alain DUBUC	Sûreté du Québec
Stephan DENIS	Canadian Police College
Ray ARCHER	Canadian Bankers Association
Arni STINNISSSEN	OPP
Bessie PANG	Society for Policing Cyberspace (by phone)

Items discussed included the CIRA change of policy, Presentation on BOTNET national strategy, finalization of resolutions, Strategic Direction, CDN Centre of Excellence for High Tech Crime, CDN Police Research Centre. Full Meeting minutes available in this report as Appendix “C”.





## **SUMMARY OF INITIATIVES/ACTIVITIES 2005/2006:**

- Identified and drafted resolutions
- Identified standardized training
- Broadened membership to include Quebec
- Initial discussions on Certification
- Communication with CIRA (Canadian Internet Registry Association) and CECA (Canadian Electronic Crime Association)
- Identification of growth trends and issues

The committee is aggressively addressing its 5 goal Strategic Plan to assist in its mandate and the following accomplishments have been made over the past 12 months.

### **Goal 1:**

#### **To Establish A Leadership Role In The Development Of Administrative Policy And Standards For Technology-Based Investigations.**

- Identified minimum standardized training
  - Created and submitted resolution to Board of Directors
  - Inclusion of Canadian Police College representation on this committee
  - RCMP creation of understudy program
- Committee endorsed RCMP developed Best Practices outreach
  - Distribution of Best Practices document
  - Distribution of Understudy Program
  - Distributed First Responders Guide to Electronic Crime
- Monitor 'who does what' nationwide, how resources are allocated
- Continue to identify the impact of e-crime on every investigation in Canada which impacts law enforcement resources and subsequent inability to be able to respond to all requests for services.
- Monitor Ontario's Child Exploitation initiative.
- Continue to educate various government levels on the impact of e-Crime and the need for proper allocation of resources in e-Crime

### **Goal 2:**

#### **The Promotion of Inter-Agency Cooperation In The Detection And Investigation Of Computer Based Crime**

- Monitor success and expansion of CETS which is a model of success as a tool for other e-Crime investigations and tool for cross jurisdictions issues
- Examination of RECOL and role/function within this committee
- Continued linkage with other CACP committees such as Law Amendments, POLIS
  - Resolution requesting minimum sentencing for Child Luring created and submitted to Board of Directors

- Consultation with Federal/Provincial/Territorial Working Group on Cyber crime in regards to proposed changes to section 372 to address new forms of communication Cyberbullying
- Monitor 'who does what' nationwide, how resources are allocated
  - Use and maintenance of 24/7 e-crime contact list prepared by Federal government
- Inclusion of Canadian Police College representation on this committee
- Identification of specific training courses in collaboration with Canadian Police College
  - Presentation on RCMP Understudy Program
- Identification of appropriate International conferences
- Support for National Strategy on Federal BOTNET project

**Goal 3:**

**The Establishment of Training Standards**

- Identified minimum standardized training
  - Created and submitted resolution to Board of Directors
  - Inclusion of Canadian Police College representation on this committee
  - Support for RCMP understudy program
- Identification of specific training courses in collaboration with Canadian Police College
- Identification of appropriate International conferences

**Goal 4:**

**The Facilitation of Public Education on Information Security**

- Ontario in collaboration with OPP, continues to distribute Internet Safety software product (LiveWires Inc.) throughout school system, beginning in January 2006 with completion in Fall 2006.
- Identification of Phishing and BOTNET's as major security issues
- Groundwork of Phishing and Wireless crime prevention articles prepared for the submission to the CACP with intentions of future public education.

**Goal 5:**

**Linkages with other CACP committees to consider new legislation in respect to e-Crime**

- Resolutions proposed in 2006 dealing with minimum training standards and minimum sentencing provisions for child luring.
- Committee members fully engaged in Lawful access consultation including subgroups identifying e-Crime committee concerns.

## **SUMMARY OF RESOLUTIONS**

### *Resolution on Training in Computer Forensics Commentary*

Since the creation of information technology, digital information or data is used in the everyday lives of all Canadian citizens and businesses. Data is stored on a variety of media and is invisible to the naked eye and for all intents and purposes, intangible. The range of electronic criminal opportunities is extensive and will continue to expand in tandem with technological advances in online communications and access. As more Canadians and Canadian enterprise conduct business on-line, data containing personal biographical information and corporate secrets become susceptible to unauthorized access by inside employees and attacks from the outside. The forensic examination of digital evidence by untrained, partially trained or self-trained investigators who do not follow validated search and seizure methodologies creates huge risk for the Canadian law enforcement community which may reduce public confidence in the investigative capability of police agencies, undermine procedural fairness and may serve to bring the administration on justice into disrepute. In some provincial jurisdictions it is the responsibility of the police organizations to provide services according to their level of classification therefore mandating more duty and accountability. The Canadian Police College provides training courses which are necessary to enable all police organizations to provide such services and therefore must be properly funded and equipped to provide computer forensics training in both official languages as required, at a minimum of once a year.

#### **Media Lines**

- Electronic crime has become an issue of national and international significance that demands the attention of law enforcement agencies and the criminal justice system.
- Forensic examination of digital evidence by untrained, partially trained or self-trained investigators who do not follow validated search and seizure methodologies creates huge risk for the Canadian law enforcement community
- Although standardized training programs exist, disparities exist amongst Canadian law enforcement agencies in the application and enforcement of standardized training for computer forensic investigators
- It is the recommendation of the CACP that all member agencies undertaking computer related search, seizure and forensic examinations undertake these functions only with personnel who

have met, at a minimum, the recommended training standards of the Canadian Police College Technological Crime Learning Institute Program or other validated training.

- The Canadian Police College provides training courses which are necessary to enable all police organizations to provide such services and therefore must be properly funded and equipped to provide computer forensics training in both official languages as required, at a minimum of once a year.

## RESOLUTION

2006

### **Computer Analysis Forensic Training**

*Submitted by the e-Crime Committee*

**WHEREAS** Canadians have connected to the Internet and embraced computer related technologies at one of the highest rates in the world, and;

**WHEREAS** electronic crime has become an issue of national and international significance that demands the attention of law enforcement agencies and the criminal justice system, and;

**WHEREAS** to address these demands the Canadian Association of Chiefs of Police formed the e-Crime Committee in 2002 with the mandate of this Committee to establish a CACP leadership role in the development of administrative policy and standards for technology-based investigations, the promotion of inter-agency cooperation in the detection and investigation of internet-based crime, the establishment of training standards and the identification of effective cooperative strategies to combat e-Crime at a local, Provincial, Canadian and International level, and;

**WHEREAS** the committee has addressed in its Strategic Plan to establish a leadership role in the development of administrative policy and standards for technology based investigations, the promotion of inter-agency cooperation in the detection and investigation of computer based crime, and the establishment of training standards, and;

**WHEREAS** the examination of computer forensic training for Canadian law enforcement agencies by the e Crime Committee has revealed that while specific standardized training programs exist, that disparities exist amongst Canadian law enforcement agencies in the application and enforcement of standardized training for computer forensic investigators, and;

**WHEREAS** the forensic examination of digital evidence by untrained, partially trained or self-trained investigators who do not follow validated search and seizure methodologies creates huge risk for the Canadian law enforcement community which may reduce public confidence in the investigative

capability of police agencies, undermine procedural fairness and may serve to bring the administration on justice into disrepute,

**WHEREAS** the Canadian Police College has developed and validated computer forensic based training courses that are delivered by the Canadian Police College and available to all accredited law enforcement agencies, and;

**WHEREAS** the Canadian law enforcement community has accepted the Canadian Police College Technological Crime Learning Institute training courses as the “standard” for computer forensic investigators, and;

**WHEREAS** the CACP e-Crime Committee has endorsed the Canadian Police College Technological Crime Learning Institute Training Program as the basis for all Canadian law enforcement personnel undertaking computer forensic investigations, further that the CACP e-Crime Committee recommends that such training be delivered in such a manner as to facilitate learning and qualification in both official languages.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police recognize the current training at the Canadian Police College for computer forensic investigators, as being an approved agency to provide training in computer forensic examination for Canadian law enforcement agencies. Which recognition does not restrict CACP member law enforcement agencies from acquiring additional forensic computer training, as would support the investigative function in the furtherance of the common goal, of thorough, comprehensive and impartial e-Crime investigations in the best interests of the Canadian administration of justice and;

**BE IT FURTHER RESOLVED** that the Canadian Association of Chiefs of Police mandates that all member agencies undertaking computer related search, seizure and forensic examinations undertake these functions only with personnel who have met, at a minimum, the recommended training standards of the Canadian Police College Technological Crime Learning Institute Program or other validated training.

## *Resolution for Minimum Sentence for Luring Offences Commentary*

Bill C-2 constitutes the Government’s response to a wide variety of recently articulated public concerns. Following Bill C-2 amendments, an adult’s sexual contact with someone anyone over 14, but under 18 will also constitute an offence where the relationship is “exploitative of the young person.” The maximum available penalty is increased from five to ten years’ imprisonment and minimum penalties are imposed. At the same time, the maximum penalties for convictions under section 215 (failing to provide necessities of life) and section 218 (abandoning a child) are increased from two to five years. Bill C-2 does not address the offence of luring under s. 172.1(1) which is an obvious form of

exploitation of children. However, many of the predicate offences involved in luring do now have mandatory minimum sentences.

## Media Lines

- Bill C-2 constitutes the Government’s response to a wide variety of recently articulated public concerns.
- The preamble to Bill C-2 recognizes that Canada has “grave concerns regarding the vulnerability of children to all forms of exploitation, including child pornography, sexual exploitation, abuse and neglect”.
- The increased penalties noted above reflected that concern. For those offences where mandatory minimums were imposed, conditional sentences are no longer available
- The offence of luring under s. 172.1(1) is an obvious form of exploitation of children yet was not addressed in Bill C-2.
- The offence of luring is a serious form of child exploitation and the penalties should reflect the significance of the charge.

## RESOLUTION

2006

### **Minimum Sentencing for Luring Section 172.1 (2) Criminal Code of Canada**

Submitted by the e-Crime Committee

**WHEREAS** With the proclamation of Bill C-2 maximum penalties for offences involving the exploitation and abuse of children were increased and mandatory minimums imposed. The preamble to Bill C-2 recognizes that Canada has “grave concerns regarding the vulnerability of children to all forms of exploitation, including child pornography, sexual exploitation, abuse and neglect”. The increased penalties noted above reflected that concern. For those offences where mandatory minimums were imposed, conditional sentences are no longer available;

**WHEREAS** The offence of luring under s. 172.1(1) is an obvious form of exploitation of children yet was not addressed in Bill C-2. However, many of the predicate offences involved in luring do now have mandatory minimum sentences. As well, for those that are hybrid offences, most now carry a maximum summary penalty of eighteen months.

**WHEREAS** The offence of luring is a serious form of child exploitation and the penalties should reflect the significance of the charge. The same policy concerns which lead to the imposition for mandatory minimums and increased maximums in Bill C-2 are equally applicable to the offence of luring.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police calls upon the Government of Canada through the Minister of Justice and Attorney-General to amend the Criminal Code to Amend s. 172.1(2) (b) of the *Criminal Code* to provide for a maximum sentence of eighteen months for a summary offence; Amend s. 172.1(2) (a) and (b) to provide for mandatory minimum sentences of imprisonment.

## **ACTIVITIES PLANNED/SIGNIFICANT DATES**

### **2006/2007 :**

August 21, 2005	Regular Committee Meeting Ottawa, Ontario
January 19, 2006	Winter Meeting, Montreal, ON
May 19, 2006	Spring Meeting, Edmonton, AB
August 19, 2006	Regular Committee Meeting St. John's, Newfoundland
Winter 2007	Regular Committee Meeting Vancouver, TBD
Spring 2007	Regular Committee Meeting Location TBD
August 2007	CACP Annual Conference Location TBD

- In 2006 the CACP E Crime Committee submitted a resolution to ensure the determination of a training standard for all technological crime forensic investigators.
- In 2006/2007 the Committee will examine new trends and issues such as BOTNET's, Cyberbullying, PHISHING, Wireless technology among others and determine suitability of resolutions or other solutions to assist Canadian Law Enforcement`



## **COMMITTEE MEMBERS LIST:**

### **CHAIRPERSON**

#### **Ken C. Smith**

Chief Superintendent  
Ontario Provincial Police  
777 Memorial Avenue  
Orillia, ON L3V 7V3  
Phone: (705) 329-6315  
Fax: (705) 329-6318  
Email: ken.c.smith@jus.gov.on.ca



**Bio:** Ken Smith joined the OPP in 1978 and was stationed at Belleville Detachment. He served in a uniform and General Law Enforcement plainclothes capacity working closely with the Tyendinaga First Nations Police Service.

In 1988 he was promoted to Corporal and accepted a position with the Anti-Rackets Branch in Toronto, subsequently serving as Detective Sergeant and Detective Staff Sergeant investigating major frauds and allegations of political corruption with ARB.

In 1994 Ken became a member of the Criminal Investigation Branch as a Detective Inspector and was assigned to investigate homicide and Major Cases throughout the province.

In 1997 Ken accepted a position as the Deputy Director of the Investigations Section of the Alcohol and Gaming Commission of Ontario overseeing both criminal and regulatory investigations in relation to legalized gaming in Ontario.

In 2002 Ken was assigned as the Bureau Commander of the Professional Standards Bureau overseeing criminal, WDHP and Police Service Act investigations for the Force's 7400 employees.

In 2004 Ken was promoted to the rank of Detective Chief Superintendent Bureau Commander of the Investigation Support Bureau and oversees the Technical Support Section, Behavioural Sciences Section, Forensic Identification and Photographic Services Section and the e-Crime Section of the Investigations/Organized Crime Command. Most recently, Ken was appointed to Regional Commander, responsible for all OPP policing duties in the Central Region.

Ken holds a Bachelor of Arts Degree from Queens University and in 2001 graduated from the inaugural course of the Police Leadership Program offered by the OACP and the University of Toronto, Rotman School of Management.

## MEMBERS

### **Ray Archer**

Canadian Bankers Association  
888 Birchmount Rd., 6<sup>th</sup> Floor  
Scarborough, ON. M1K5L1  
Telephone: (416)-615-4557  
Fax: (416)-615-5178  
Cell: (416) 371-5845  
Email: [ray.archer@scotiabank.com](mailto:ray.archer@scotiabank.com)



CANADIAN BANKERS ASSOCIATION  
ASSOCIATION DES BANQUIERS CANADIENS

*Building a Better Understanding / Pour mieux se comprendre*

**Bio:** Ray is the Vice President & Deputy CISO of Information Security & Control at Scotiabank. His global responsibilities include: Security Operation Services (Change Control & UserID Administration), Vulnerability Management (Server & Desktop Security), Cryptographic Services, Technical Security Services (Network Security Center) and Security Intelligence and Forensic Services. Ray's previous post with Scotiabank was the Director of Technological Crime and Forensics - Corporate Security at Scotiabank. Between his careers with the Royal Canadian Mounted Police (RCMP) and Scotiabank he has gained over 31 years of investigational, technical and audit experience in the areas of criminal investigations, information technology and electronic data processing auditing. He has extensive experience in computer forensics, information security systems analysis, and provides a consultative role as an IT security specialist to all areas within the Scotiabank Group.

Ray joined Scotiabank in 1998 after serving 23 years with the RCMP. IT investigative and forensics experience was gained by various assignments, duties and formal education over the past 28 years. As a member of the RCMP - Security Evaluation and Inspection Team (SEIT), he performed IT audits on Federal Government departments processing highly sensitive information, as well as, providing a consultative role as an IT security specialist. Ray received a B.A. Degree from University of Manitoba and holds the Certified Risk Professional (CRP) and Certified Information Systems Security Professional (CISSP) designations. Ray is a member of the Computer Security Institute and is a security advisor to the Bank Administration Institute (BAI).

**Richard C. (Dick) Bent**

Chief Superintendent  
Deputy Criminal Operations Officer - Federal  
Royal Canadian Mounted Police “E” Division  
Vancouver, B.C.  
Telephone: 604 264-2200  
Fax: 604 264-3229  
Email: [dick.bent@rcmp-grc.gc.ca](mailto:dick.bent@rcmp-grc.gc.ca)



**Bio:** Born in Saskatchewan, Dick Bent joined the RCMP in 1974. After completing basic training he was transferred to Alberta where he served in a variety of roles for twenty years.

After working in general duties and traffic roles in a number of detachments throughout Alberta, he was transferred to Division Headquarters in Edmonton where he worked in the Complaints and Internal Investigation Section and then Major Crimes as a Team Leader.

In 1993 Dick was transferred in charge of a Sub/Division General Investigation Section responsible for all serious crime investigations in the Peace River region of Alberta.

In 1994, he was promoted to the rank of Inspector in Nova Scotia where he worked in planning the 1995 G7 Summit in Halifax, in the Staffing and Personnel Section, and finally as the Officer In Charge of the Federal Policing Branch for the Province of Nova Scotia.

In 1997, he was transferred to the RCMP National Headquarters in Ottawa where he gained exposure in a number of areas including the Finance, Commissioner’s Secretariat, Criminal Intelligence, and Community, Contract and Aboriginal Policing Directorates. He then worked for two years in Executive/Officer Development and Resourcing.

In 2002, Dick was promoted to the rank of Chief Superintendent and transferred to his current position as the Deputy Criminal Operations Officer in British Columbia responsible for all Federal Policing in the province.

## **Alain Dubuc**

Lieutenant  
Chief of Division  
Computer Crime Division  
Electronic and Informatic Surveillance Service  
Sûreté du Québec  
1701 Parthenais Street  
Montreal, PQ H2K 3S7  
Phone: (514) 598-4098  
Fax: (514) 596-3086  
Email: [alain.dubuc@surete.qc.ca](mailto:alain.dubuc@surete.qc.ca)



**Bio:** Alain joined the S.Q. in 1991 as a patrol officer. In 1996, he became a major crime investigator attached to the Commercial and Business unit at headquarters in Montreal. He is an experienced investigator dealing with corruption, credit card and fraud culminating in computer crime investigations until 1999.

In 1999 the SQ created a new Tech Crimes Division where he was assigned as a major crime investigator until 2002 working on various investigations including child pornography cases.

In 2002, he was promoted to Staff Sergeant and was the assistant to the chef of the Tech Crimes Division in Montreal in charge of all operations and investigations. In early 2005, he was promoted to Lieutenant and placed in charge as Chef of Division. His responsibility includes managing staff of the unit in Quebec City and the Division of Montreal and keeping good relationship with all law enforcement agencies and private partners.

## **Steve Izzett**

Staff Inspector  
Unit Commander, Intelligence Services  
Toronto Police Service  
40 College Street  
Toronto, Ontario  
M5G 2J3  
(416)808-3513  
Fax: (416) 808-3502



**Bio:** Steve joined the Toronto Police Service as a cadet in 1983 and is married with two children. He has a bachelor of arts in Political Science from the University of Toronto.

Steve has a diverse skill set and worked in the following areas of the Toronto Police Service: 42 Division, 41 Division, 14 Division, Emergency Task Force, Homicide Squad, Fraud Squad, Staff Development, Proceeds of Crime, Court Services, Professional Standards, Corporate Planning and is currently the Unit Commander of Intelligence Services. He has spent approximately 7 years in various squads - the majority of this time being spent in the Fraud Squad and Proceeds of Crime.

Steve received training in computer crime at the Canadian Police College (Level 1, 2 and 3) in the early 1990's and utilized this knowledge conducting examinations on hard drives while assigned to the Fraud Squad. This was prior to the creation of the Tech Crime Unit.

### **David Korol**

Superintendent,  
Special Investigations Division  
Edmonton Police Service  
9620-103 A. Avenue  
Edmonton, Alberta, Canada T5H 0H7  
Business: (780) 421-3357  
Fax: (780) 421-3345  
Email: [david.korol@police.edmonton.ab.ca](mailto:david.korol@police.edmonton.ab.ca)



Bio: Superintendent David KOROL had 26 years experience with the Edmonton Police Service. Throughout his career Superintendent KOROL has worked in a variety of roles and ranks within Patrol, Forensic Identification Services, Criminal Investigation Section, Human Resources, Special Projects, Chief's Executive Assistant and Special Investigations. Superintendent KOROL has a Bachelor of Arts degree from the University of Saskatchewan and a Public Administration certificate from the University of Alberta.

Superintendent KOROL is currently in charge of Special Investigations Division and oversees the Organized Crime Branch and the Intelligence Support Branch, which houses a Technological Crimes Unit. Although Superintendent KOROL does not have extensive formal computer training, he is able to help link operational needs with technological realities, and serves as a steering committee member for numerous Edmonton Police Service computer based projects.

## Réal Laguë

Inspector  
Chief of Service,  
Electronic and Informatic Surveillance Service  
Sûreté du Québec  
1701 Parthenais Street  
Montreal, PQ H2K 3S7  
Phone: (514) 598-4613  
Fax: (514) 596-3086  
Email: [real.lague@surete.qc.ca](mailto:real.lague@surete.qc.ca)



**Bio:** Mr. Réal Laguë has been an officer with the Sûreté du Québec for 26 years. He holds the rank of Inspector and is currently the Chief of the computer and electronic surveillance service.

Inspector Laguë has been with criminal investigations support services since September 1997. Since June 2001, he has been the manager of the Sûreté du Québec's computer and electronic surveillance section. His section is responsible for the following services, among others: interception of private communications, design and installation of equipment for interception of private communications, computer search and seizure and their forensic examination for court purposes, as well as network security and electronic countermeasures.

## Bessie Pang

Executive Director  
The Society for the Policing Of Cyberspace (POLCYB)  
Suite 480 - 2755 Lougheed Highway,  
Port Coquitlam, B.C., V3B 5Y9  
Telephone: (604) 927-1962  
Fax: (604) 927-1955  
Cell: (604) 671-7689  
Email: [polcyb@telus.net](mailto:polcyb@telus.net)



**Bio:** Pang is a Criminology Consultant. Ms. Pang moved to Canada from the United Kingdom after receiving her B.A. Hons. in "Developmental Psychology with Cognitive Studies", which focused on Psychology and Artificial Intelligence programming. After completing her M.A. Degree in Criminology in Vancouver, Ms. Pang has been working in various fields of Criminology. While working at the BC Forensics Psychiatric Commission in Vancouver and the National Headquarters of Correctional Services Canada in Ottawa, Ms. Pang specialized and published research in profiling risks/needs of juvenile and adult sex offenders, women offenders, and dangerous offenders.

Since returning to Vancouver from Ottawa, Ms. Pang established Primexcel Enterprises Inc. to conduct Criminology and other business consultations. Ms. Pang was commissioned by the B.C. Forensic Psychiatric Commission to develop the first comprehensive “Standards and Guidelines for the, Assessment, Treatment and Management of Sex Offenders in B.C.” Ms. Pang also has extensive experience in policy development; development of provincial and federal standards, including staff training and equity employment; programme development and evaluations – including programmes for youth gangs, community policing, and domestic violence.

Ms. Pang is one of the founders of The Society for the Policing of Cyberspace (POLCYB) – an International Society based in Vancouver, B.C. Currently, in addition to other consultation projects, Ms. Pang also is assuming the role of the Executive Director of POLCYB.

**Tom Pownall, MBA**

Superintendent  
OIC - Technological Crime Branch  
RCMP Technical Operations  
St. Joseph Blvd.  
Ottawa, ON K1A0R2  
Telephone: 613 998-6066  
Fax: 613 993-2963  
Email: [tom.pownall@rcmp-grc.gc.ca](mailto:tom.pownall@rcmp-grc.gc.ca)



**Bio:** Tom joined the RCMP in 1985 and followed basic training with an assignment to RCMP Federal Sections in Ottawa, Ontario. Following service in General Investigations Section and Traffic Section, he was transferred to Commercial Crime Section as a fraud investigator in 1988. In 1992 he was transferred to a position as a computer crime investigator with the Commercial Crime Section. Since that time he has held different positions in Technological Crime, including OIC - Policy and Program Management and he is currently the Officer-In-Charge of the national technological crime program. Tom currently represents the RCMP on the G8 High Tech Crime Working Group.

Tom holds a Master of Business Administration from Concordia University, a Bachelor of Arts from McGill University and a Certificate of Management Practices from Concordia University. He also holds a Certificate in General Police Studies and Certificate in Advanced Police Studies from the Canadian Police College.

**Paul L. Roy**

Inspector,  
Criminal Investigation Division,  
Ottawa Police Service  
474 Elgin Street,  
Ottawa, Ontario  
K2P 2J6  
Phone # (613) 236-1222 extension 5469  
Fax # (613) 760-8122  
Email: [roy@ottawapolice.ca](mailto:roy@ottawapolice.ca)



Bio: Inspector Paul Roy has been a member of the Ottawa Police Service since 1975 and is presently the Officer in charge of the Criminal Investigative Branch dealing with Property & Enterprise Crimes and Investigative Support. The Branch includes the High Tech Crime Unit, Firearms Unit, Polygraph Unit, the Organized Fraud and Auto theft Units, as well as the Forensic Identification Section.

Throughout his career; Inspector Roy has worked in a variety of roles and ranks within Patrol Operations, Criminal Investigations, Professional Standards, and Human Resources Sections. Notably, in 1996-97, Inspector Roy served as the Acting Chief of Police for the Hawkesbury Police Service and in 2001; he was seconded to the Human Resources Directorate of the Royal Canadian Mounted Police.

In 1993, Inspector Roy graduated from Carleton University, obtaining a Certificate in Law Enforcement Studies.



## *Associate Corporate Member*

### **Michael Kert Eisen**

Vice-President, Law and Corporate Affairs  
Microsoft Canada  
1950 Meadowvale Blvd., Mississauga, ON, L5N 8L9  
Telephone: 905-363-8430  
Fax: 905-363-0973  
Cell: 416-434-3737  
Email: [meisen@microsoft.com](mailto:meisen@microsoft.com)



Bio; As Vice-President, Law and Corporate Affairs at Microsoft Canada Co., Michael Eisen is a member of the company's Canadian Leadership Team which is responsible for driving the company's long-term business direction and future growth. He oversees Microsoft Canada's legal needs generally with particular emphasis on government relations, competition policy and intellectual property issues. Mr. Eisen comes to Microsoft Canada from a prominent Toronto legal firm where he was Secretary and General Counsel to the Canadian Alliance Against Software Theft and Microsoft's lead Canadian outside counsel. Mr. Eisen is a member of the Canadian Bar Association, the Law Societies of Alberta and Upper Canada, and the Licensing Executives Society. Educated at York University and Osgood Hall Law School he was admitted to the Ontario Bar in 1977 and the Alberta Bar in 1981.

## Technical Advisors

### **Susheel Gupta**

Federal Prosecutor/Computer Crime Advisor  
Department of Justice Canada,  
284 Wellington Street, EMB 2061,  
Ottawa, ON, K1A 0H8  
Telephone: (613)-941-8517 (24 hours)  
Cell: (613)-941-8517  
Email: [sush@justice.gc.ca](mailto:sush@justice.gc.ca)



Department of Justice  
Canada

Ministère de la Justice  
Canada

**Bio:** Susheel Gupta is currently a Federal Prosecutor with the Department of Justice in Canada. Specifically, he has been designated the Computer Crime Advisor for the prosecution unit Ottawa. Sush is a Computer Crime Advisor who currently assists on prosecutions and investigations with the Federal, Provincial and Local governments and institutions. Sush is a director of POLCYB (The Society for the Policing of Cyberspace), publishes a daily Computer Crime Newsletter, and regularly instructs on the legal aspects of Cyber crime at the Canadian Police College. Sush is also a Training Coordinator for FPS on Computer Crime and works with the Department of Justice, the Federal/ Provincial/ Territorial Working Group on Cyber crime, and is a Canadian designate to task forces on Cyber crime with the FBI and the Secret Service. Sush is also an advocate for Internet Safety and presents many training sessions and presentations on the topic across Canada.

### **Dan MacRury**

Senior Crown Attorney  
Public Prosecution Service  
Government of Nova Scotia  
Maritime Centre  
Suite 1325  
1505 Barrington Street  
Halifax, NS B3J 3K5  
Telephone: 902 424-8734  
Fax: 902 424-0659  
Email: [macrurda@gov.ns.ca](mailto:macrurda@gov.ns.ca)



**Bio:** Mr. MacRury, a native of Sydney, Nova Scotia joined Nova Scotia Legal Aid in 1989 and before that was in private practice. He was admitted to the bar in 1986. He is a graduate of St. Francis Xavier University in Antigonish and the University of New Brunswick Law School in Fredericton. Mr. MacRury was appointed as Crown Attorney in 1996 assuming responsibilities in the Cape Breton Region. Mr. MacRury was transferred to Halifax in 1998 where he continues to practice today.

Mr. MacRury is a member of the Federal/Provincial/Territorial Working Group on Cyber crime and is well versed in the complex legal issues that have arisen since digital evidence has been introduced into the judicial system. Mr. MacRury is the Vice-President of the Canadian Criminal Justice Association.

## Gareth Sansom

Director, Technology and Analysis  
Lawful Access Group,  
Criminal Law Policy Section  
Department of Justice Canada,  
284 Wellington Street, EMB 2061,  
Ottawa, ON, K1A 0H8  
Email: GSansom@JUSTICE.GC.CA



Department of Justice  
Canada

Ministère de la Justice  
Canada

**Bio:** Gareth has been a policy advisor in the Canadian federal government since 1990. His work has always dealt with advanced communications networks, often involving public safety questions, in the context of which he has conducted research on the issues of obscenity and child pornography online. Gareth was the author of Industry Canada's public discussion paper *Illegal and Offensive Content on the Information Highway* (released June 1995), which was one of the first public Canadian government documents to deal with the question of child pornography and obscene material on the Internet. Prior to joining the Department of Justice Gareth was with the Electronic Commerce Task Force at Industry Canada where he was senior advisor in cryptography policy.

In 2001, Mr. Sansom received a Recognition Award from the Deputy Minister of Justice in acknowledgment for "exceptional dedication and extraordinary efforts in developing the Government of Canada's policy and legislative proposals to respond to the decision of the Supreme Court of Canada in the case of *Regina v. Sharpe* (2001)", a case challenging the constitutionality of Canada's *Criminal Code* provisions regarding the possession of child pornography.

Gareth received his B.A. Honours from Trent University and an M.A. in Communications from McGill University where he also undertook doctoral studies. Gareth has taught a variety of university courses in Mass Communications at Carleton University including courses on post-industrial society and information security.

Gareth's current work with the federal department of Justice is focused on high-tech crime issues including child pornography on the Internet, as well as the technical and legal aspects of lawfully authorized electronic surveillance.



## Alex Smith

Director, Law and Technology  
Crown Law Office – Criminal (Ont.)  
9th Floor, 720 Bay Street,  
Toronto, Ontario, M5G 2K1  
Phone: (416) 212-1166  
Email: [alexander.smith@jus.gov.on.ca](mailto:alexander.smith@jus.gov.on.ca)

Bio: Alex Smith (B.A., M.A., L.L.B.) is currently the Director of Law and Technology for the Ministry of the Attorney General, Criminal Law Division. Upon graduating from the University of Windsor Law School in 1981, Alex was named to the Dean's Honour Roll, and was the recipient of the CCH Prize for Legal Writing. Alex completed his Articles at the Office of the Crown Attorney in London. Following his call to the Bar in 1983, he was hired as an Assistant Crown Attorney in Lindsay. In 1986 he transferred to the Brampton Crown's Office and in 1989 joined the Guelph Crown Attorney's Office where he remained until 2001 at which time he was appointed to his current position.

In his current position, Alex manages information technology issues for the Criminal Law Division. He Chairs the Attorney General's Task Force on Internet Crimes Against Children and the Division's e-Disclosure Committee and participates in a number of other committees at the provincial and federal levels. Alex has organized and participated in numerous educational programs as a panellist or lecturer and is a frequent speaker at continuing legal education programs. In addition to the responsibilities associated with his current position, Alex continues to represent the Crown in all levels of trial and appeal courts.

## Arni Stinnissen

Detective Staff Sergeant  
Manager- OPP e-Crime Section  
777 Memorial Ave.,  
Orillia, ON L3V 7V3  
Phone: (705) 329-6441  
Fax: (705) 329-6318  
Email: [Arni.Stinnissen@jus.gov.on.ca](mailto:Arni.Stinnissen@jus.gov.on.ca)



Bio: Staff Sergeant Stinnissen is a senior police officer with over 27 years of experience with the Ontario Provincial Police. In years gone by, he worked in the Computer Services Branch of the OPP in Toronto where he was a systems officer providing maintenance on the Tandem mainframe system. He also provided help desk duties supporting the OPP's early growth in the computer area. Staff Sergeant Stinnissen was also project leader for the Anti-Rackets Section document imaging system.

Staff Sergeant Stinnissen is the Manager of the Electronic Crime Section, which handles reported computer-based crime for the OPP and other clients such as municipal police services and government

agencies. Staff Sergeant Stinnissen is a regular speaker in the police community on topics such as search and seizure, electronic evidence and information age crime. Staff Sergeant Stinnissen has successfully completed numerous computer-based courses from the Canadian Police College and was a part-time professor at Georgian College for their Cyberspace Security Program. Staff Sergeant Stinnissen is also a member of the FPT/WG on Cyber crime.

### **France Thibodeau**

Coordinator, Computer Studies  
Canadian Police College  
P.O. Box 8900  
Ottawa, Ontario  
K1G 3J2  
Phone: (613) 990-2480  
Fax: (613) 990-9738  
Email: [fthibode@cpc.gc.ca](mailto:fthibode@cpc.gc.ca)



Bio: France Thibodeau is a civilian member of the Royal Canadian Mounted Police. She has been the Manager of the Technological Crime Learning Institute at the Canadian Police College for more than ten years.

Ms. Thibodeau leads a team of eleven high-tech crime specialists consisting of RCMP Police officers and civilian members. Her team has trained thousands of police officers from across the Canada and countries from around the globe.

Ms. Thibodeau has a Bachelor of Science degree in Computer Science from the University of New Brunswick. Over the past decade, she has devoted significant time and effort to continuous learning in order to stay current in the fields of computer forensics, on-line investigative techniques, and in the latest adult learning techniques.

## Appendix "A"

### Minutes of e-Crime Committee Meeting CACP e-Crime Committee August 21st, 2005 Ottawa, ON – Westin Hotel

<u>Members participating</u>	<u>Organization</u>
Ken SMITH (Co-Chair)	OPP
Doug LANG (Co-Chair)	RCMP
Ray ARCHER	CBA
Dick BENT	RCMP
Mike EISEN	Microsoft
Jim RAMER	Toronto Police
Alex SMITH	Attorney-General Ontario
Arni STINNISSSEN	OPP

<u>Regrets</u>	<u>Organization</u>
David KOROL	Edmonton Police
Dan MacRury	Public Prosecution, Nova Scotia
Susheel GUPTA	Justice Canada
Bessie Pang	POLCYB
Réal LAGUË	Sûreté du Québec
Alain DUBUC	Sûreté du Québec
Gareth SANSOM	Justice Canada

#### 1. Opening Remarks

There was a round of introductions and a special welcome to our new members, Chief Superintendent Dick BENT from the RCMP, Ray ARCHER representing the Canadian Bankers Association and Jim RAMER representing the Toronto Police. K. Smith apprised the members of the report that was submitted to the CACP Board of Directors earlier that day. The Board recognized the valuable contributions that this committee was making and supported the committee meeting 3 times a year. K.SMITH also advised the members that the Board has approved financial assistance of \$5,000.00 that can be used to offset meeting expenses.

#### 2. Review of Membership

The e-Crime Committee discussed membership and noted that there was a lack of law enforcement representation from the east coast. Dan MacRURY to be tasked with making suggestions as to membership ideas in this regard. Since the resignation of Ruth Sutton from the Bank of Montreal, there is a recommendation that Iouri Petoukov be contacted and invited to the next meeting in December.

Committee members also wondered if there was any interest in membership from Montreal Urban police and would be asking LAGUË to explore this item further.

Action item: MacRURY  
Action item: STINNISSSEN  
Action item: LAGUË

### **3. Review of Previous Minutes**

The previous minutes of June 2/3, 2005, were reviewed and approved.

### **4. Review of Action Items**

Report on Action Item – Membership

Completed and new members in attendance, other members identified and further recruitment in progress

Report On Action Item – Electronic copy of First Responders Guide

Completed. Upon request of the e-Crime committee members and other LE agencies, the RCMP Best Practices document and guide can be used as templates, including removal of RCMP logos etc. It would be appreciated if the proper acknowledgements were made.

Report on Action item – RECOL

Completed. Presentation to membership later in meeting

### **5. Response to CIRA proposals**

As per the previous meeting minutes, Stinnissen advises that a letter outlining the position of the CACP e-Crime committee has been sent to the Canadian Internet Registry Association (CIRA). This was in regards to their proposed policy changes. Since the last meeting in June, the committee has learned that CIRA has moved quickly ahead of schedule on their policy changes and not implemented or addressed any of the concerns voiced by law enforcement. Committee members wondered whether or not the proposed lawful access changes would address the committee's concerns. Committee members would be requesting a presentation from the CACP Law Amendments Committee to address these changes.

Action item: STINNISSSEN to acquire speaker for December meeting.

### **6. Computer Forensic Training**

France Thibodeau from the Canadian Police College provided a presentation on the college's mandate in providing advanced and specialized training in management and law enforcement related to organized crime and multi-jurisdictional crime to all Canadian police officers which includes providing advanced training in computer crime and cybercrime investigative techniques. Consists of a staff of 7 people, which includes a mix of regular police officers and civilian specialists. The also enlist private sector

experts for certain topics. Course offerings range from computer search and seizure to network intrusion investigations. 8 Core Courses:

Computer Forensic Examiner  
Network Principles and Investigative Techniques  
Cybercrime Investigative Techniques  
Linux Forensic Techniques  
Macintosh Electronic Search and Seizure  
Network Intrusion and Incident investigation  
Canadian Internet Child Exploitation Course  
Using the Internet as an Intelligence Tool

CPC also offers:

3 Online (distance learning) courses  
Internet Searching Techniques, Basic, Intermediate, and Advanced

CPC also offers:

2 Workshops, Designed to update high-tech crime investigators on new technology and new techniques  
Advanced Macintosh Forensics  
Wireless Network  
2 Courses under development  
Online Undercover Course (ICE Units)  
Log Analysis Course

CPC also collaborating with the RCMP in developing a Technological Crime Understudy Program  
Designed for candidates interested in being a Technological Crime Forensic Analyst/ Investigator  
18-24 month training program

Combination of courses and on-the-job assignments

Constantly being revised

RCMP Understudy Program

During the Understudy period, the participant must successfully complete courses such as;

Computer Forensic Examiner (CPC)  
Cybercrime Investigative Techniques (CPC)  
Online Internet Searching Techniques Courses (CPC)

A+ Certification

Complete all assignments and examinations carry a diversified caseload

Submit all forensic analysis conducted to assigned coach/mentor for verification

Committee members were pleased with the presentation and agreed that the Canadian Police College would be the logical entity to partner with to achieve one of the key strategies as outlined in our long-term goals, "The Establishment Of Training Standards" and would compliment the goal of "To Establish A Leadership Role In The Development Of Administrative Policy And Standards For Technology-Based Investigations." It was agreed that France should be invited to the next series of committee meetings as we develop training standards.

Action item: LANG to continue dialogue with CPC in regards to future meetings.



## **7. Security of Information Act (SOIA)**

LANG spoke about forthcoming SOIA designations for "covert operations support" and what they mean for other law enforcement agencies outside the RCMP. The Security of Information Act (SOIA) was introduced in December 2001 and replaced the Official Secrets Act (OSA). The Act permanently binds all levels of RCMP employees who have access to special operational information to secrecy by respecting information they have become knowledgeable about during the course of their employment. The programs within RCMP Technical Operations are designated in the schedule, thus partners working with our various electronic surveillance, physical surveillance and operational support programs will require special SOIA designation. Processes for completing these designations have just been finalized. Our program managers have just started determinations of whom in other law enforcement agencies or otherwise require special designations. LANG understands that this is causing concerns amongst its partners. LANG advises that the intent of the designation to protect tools and procedures that are being used to covertly conduct investigations. LANG advises that the RCMP often is given tools from other LE agencies from around the world and among other things, this designation protects the integrity of these international contacts. An example given was that an officer in the OPP e-Crime Section could be the recipient of these tools but would be bound to secrecy in the tools use and operation during the officer's tenure with the OPP and thereafter. LANG advises that this should continue to be discussed at future meetings. A.SMITH expressed some concerns whether or not this designation would protect eventual disclosure during a criminal prosecution.

## **8. Information items**

EISEN provided an update on CETS, which has two aspects, one Canadian and the other International. The National Child Exploitation Coordination Centre (NCECC) and over 20 police services in Canada are now part of the Canadian CETS network. Due to the quality of the tool and the success in Canada, the project has gained momentum internationally with possible near term deployment in the UK and the U.S. Law enforcement agencies in Europe, Asia and Brazil are also looking closely at CETS. It is hoped that eventually there will be an international network spanning all borders.

EISEN provided an update on the BOTNET project. Numerous unsuspecting computers are remotely taken over and their combined computing power used to facilitate illegal activity including denial of service attacks and the propagation of malicious code. This poses a significant risk to the global online community. Microsoft has already organized two international conferences to discuss BOTNET's (Redmond in 2004 and Prague this past April). There is an upcoming meeting in the fall and committee member agencies can be supplied with information so that interested persons can enquire about attending. It is a highly technical training session and very valuable for those in this business.

LANG noted that the POLCYB China Conference agenda was out and available for those on the committee who were interested in going. LANG noted that Phishing attacks were on the increase but LE were under resourced to deal with these complaints and were not engaged in these investigations, which is frustrating for the financial institutions. On a priority assessment basis, Phishing schemes as well other frauds are competing against crimes against persons, including child porn and sexual assaults. There was also jurisdictional issue in that the local police should be investigating these crimes but when

they try to investigate, the perpetrators are often found to operating from offshore. ARCHER advised that the techniques for prevention of Phishing can be found on the Microsoft website. ARCHER also noted that Phishing scams in which bank clients had their accounts compromised includes the substantive criminal code offence of “unauthorized access”. A.SMITH noted that revised laws are needed that would better address privacy issues. ARCHER noted that the best weapon against Phishing is the education of the public. ARCHER noted that it would be beneficial if certain rogue IP addresses were identified and subsequently blocked from accessing Canadian IP addresses. A.SMITH noted that the ISP’s would be reluctant to do this unless there were some legal obligation for all ISP’s and protection to do so. This may also work with blocking IP addresses that have been associated with Child Porn.

Action Item: ARCHER to provide article on Phishing for CACP magazine and/or newsletter.

SMITH related his experience on the e-disclosure working group that is examining standards and best practices targeting a model for national standards. He noted that the police community is far ahead in this area.

BENT and RAMER indicated their pleasure of being on this committee and looked forward to making contributions whenever possible

STINNISSSEN provided the committee a brief presentation on RECOL. There was definite interest in this tool and a representative from the RECOL project to be invited to a future meeting.

Action Item: Invitation to be sent to RECOL project for future attendance

STINNISSSEN advised that the Spam task has produced its final report. It can be found at:  
[http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h\\_gv00248e.html](http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html)

Action Item: Web address to be emailed to all committee members

## **9. Proposals for Resolutions**

The committee has agreed that 2 resolutions be drafted for submission to the CACP Board in 2006.

- Minimum training/adequacy standards in order to provide the service of computer forensics
- Recognition of the Canadian Police College as the standard
- Blocking of Rogue Internet Protocol Addresses from accessibility from Canadian IP addresses
- Prevention of fraudulent activity from offshore
- Prevention of Child Pornography
- Protection of ISP’s who block IP addresses

Action Item: LANG to draft resolution for comment on Training

Action Item: ARCHER to draft resolution for comment on IP Blocking

## **10. Discussion on strategic Plan/Next Steps**

Focus for 2005/2006 will be on establishing standardization of training

## **11. Future Meetings**

Next meeting December 8, 2005, Montreal PQ, hosted by Réal LAGUË

### Guest Speakers

Representative from the office of Public Safety and Emergency Preparedness Canada – Critical Infrastructure Protection

Speak on mandate and e-Crime issues

Action Item: LANG

Representative from Microsoft Canada

Speak on Microsoft products and the effects for law enforcement in the future.

Action Item: EISEN

## Appendix "B"

### CACP e-Crime Committee January 19, 2006 Montreal, PQ La Sûreté du Québec

#### Members participating

Ken SMITH (Chair)  
Dick BENT  
Tom POWNALL  
Steve IZZET  
Keith WHITTON  
Mike CALLAGHAN  
Réal LAGUË  
Stephen BOUCHARD  
Francesco SECONDI  
Alain DUBUC  
France THIBODEAU  
Gareth SANSOM  
Ray ARCHER  
Arni STINNISSSEN  
Dan MACRURY  
Alex SMITH  
Bessie PANG

#### Organization

OPP  
RCMP  
RCMP  
Toronto Police  
Edmonton Police (representing David KOROL)  
Ottawa Police (representing Paul ROY)  
Sûreté du Québec  
Montreal Urban Police  
Montreal Urban Police  
Sûreté du Québec  
Canadian Police College  
Justice Canada  
Canadian Bankers Association  
OPP  
Public Prosecution, Nova Scotia (by phone)  
Attorney-General, Ontario (by phone)  
Society for Policing Cyberspace (by phone)

Regrets

Organization

Michael EISEN  
Susheel GUPTA

Microsoft  
Justice Canada

### 1. Opening Remarks

Introductions – The Committee Chair recognized the hospitality of our gracious hosts, Sûreté du Québec. SMITH also welcomed new members Tom POWNALL, RCMP and Steve IZZET from Toronto as well as new attendees BOUCHARD and SECONDI from the Montreal Urban police and WHITTON and CALLAGHAN representing members from Edmonton and Ottawa respectively.

## 2. Review of Membership

Dan MacRury reported that he has a law enforcement representative from the east coast who is interested in joining the committee. There have been some organizational changes within the Bank of Montreal as a result; someone to replace Ruth Sutton has not been identified as yet. Correspondence ongoing.

### Action item 1:

STINNISSSEN to determine representative from BMO replacing Ruth Sutton

## 3. Review of Previous Minutes

Acceptance of minutes (August 2005) (Smith)

Call for additional agenda items. MacRURY requested that an additional agenda item be considered and a resolution be put forward. MacRURY noted that the child pornography sections have been amended to include mandatory minimum sentencing. MacRURY suggests that child luring legislation be amended to include minimum sentences as well. MacRury volunteer to draft resolution.

### Action item 2:

MacRURY to draft resolution in regards to amendments to the Criminal Code asking for minimum sentencing for Child Luring offences.

## 4. Law Amendments Committee

Update from Law Amendments Committee provided by Co-chair Detective Chief Superintendent Frank Ryder

### **MITA Legislation**

Died on the order paper after being introduced Nov 15th as the result of the dissolution of parliament. The legislation will have to be reintroduced by the new government and that will depend on the priorities of the new government. Although the proposed legislation may change, LAC wanted to apprise e-Crime committee members with some concerns with the legislation that was tabled on Nov. 15th. The first concern was the silence on operational costs issues. Presumably the drafters wanted to avoid this issue because of ongoing court litigation surrounding operational costs. On haul back fees it was hoped the legislation would require telco's to push the circuits to the edge of existing networks and close to the police interception facility. The legislation only required haul back to major haul back centres, which may cause issues for police interception facilities outside of major centres. Another concern was the provisions around subscriber information. While the legislative scheme called for a warrant less system for subscriber info, the process may be too bureaucratic/process oriented.

The CACP key messages around the need for legislation are as follows:

This is not about increasing police power, but rather merely keeping up with new technology.

When and to whom the police may direct their access and intercept capabilities must, as they are now, be the subject of prior approval of the courts but the technological ability to actually implement the court ordered access must exist. There should be no ‘intercept safe havens’ in Canada.

New communications technologies are not of themselves problematic but unregulated and without the necessary checks and balances that can have unintended detrimental consequences. Modern legal mechanisms are required to ensure we as a society balance the needs of global competitiveness with that of public safety.

Modern communication technology shrinks distances and operates free of geographical constraints. Organized criminal, Internet predators and terrorists know this fact. Legislation in Canada must reflect the increasing cross border nature of crime.

### **RCMP - Telus action**

As the result of the refusal to comply with a production order on July 25th, 2005 TELE-MOBILE COMPANY (TELUS) was charged with Section 487.017 of the Criminal code. As the result of the laying of the charge TELUS is now complying with the production order. LAC is monitoring the developments of this file. The prosecution may go ahead.

### **Security of Information Act**

LAC is working with the RCMP to get some answers relating to the provisions in the Act designating individuals to be permanently bound to secrecy. The answers have just been received and are being reviewed.

### **Resolutions**

Any resolutions that have a legislative amendment should be forwarded to the LAC for review.

### **CACP Legislative Goals**

The LAC drafted a single page document (draft) that will be tabled with the CACP Board for consideration and eventual communication to the new government. The contents were shared with e-Crime Committee members.

#### CACP LEGISLATIVE GOALS — DRAFT

A Restoring public respect for the Justice System  
Re-establishing Public Confidence in Community Safety

By:

- a) Mandating serious consequences for serious crime
- b) Denouncing the culture of organized crime violence and anti-social behaviour as primarily seen in the street gangs
- c) Ensuring the application of Parliament’s legislative intention
- d) Reducing the complexity and inefficiency of the investigative and criminal trial process
- e) Reaffirming law enforcement’s operational and financial capacity to police Canadian communities

To be achieved by:

- Ensuring the appropriate legislative framework regarding bail provisions
- Establishing sentencing principles which address deterrence and public safety including eliminating the application of “dead time” sentencing
- Exacting strict consequences for crimes against the administration of justice
- Upholding the *Canadian Charter of Rights and Freedoms*
- passing of effective lawful access legislation
- Redesigning the YCJA insofar as it applies to violent offenders, repeat offenders and street gangs
- Securing Federal leadership to ensure the passage of inter-provincial police jurisdiction
- Establishing administrative or legislative rules to ensure fair and efficient trials applying to:  
Remands, adjournment and pre-trial processes  
Major trial case management  
Disclosure  
Police witness management
- Considering the financial and resource implications of operationalizing legislation

B In order to ensure the integrity and ongoing commitment to these goals:  
The convening of a National Conference including all justice system partners  
The establishment of a standing process to continue the ongoing work to  
achieve these goals

## **5. Speaker –Quebec-wide Working group Sgt. Peter Hawkins**

Sgt. Peter Hawkins, Integrated Technological Crime Unit, RCMP provided committee members a presentation of their mandate and an overview of the Annual provincial meeting of technological crime investigators and support personnel. The provincial meeting idea was developed by the ITCU of “C” Division. It is the intention of the RCMP to continue to promote partnership and spear head this initiative well into the future. The purpose of the meetings is to share information, develop a network of contacts, and develop work groups to jointly tackle common issues. At the last meeting, 16 organizations participated including;

RCMP

Justice Canada

Revenue Canada

Canada Boarder Service Agency

C.S.I.S.

Industry Canada

Department of National Defence

Revenue Québec

Montreal city tech crime

SQ tech crime support

SQ cyber surveillance team

SQ child pornography unit

Laval tech crime support

Longueuil tech crime unit  
Québec city tech crime unit  
Justice Québec

As a result of these ongoing meetings, partnerships were created with multiple organisations, there was information sharing resulting in improved service delivery to the clients of all organizations. Shared Training opportunities were explored which will enable cost savings by way of group discounts and economies of scale. Large network of contacts permits problem solving on a grand scale and possibility of cost savings through group purchases of equipment. Minimization of the duplication of effort in R&D, training, development of procedures, and investigations will be other benefits.

## **6. Resolution on Computer Forensic Training**

Tom POWNALL presented the committee with a draft resolution on standards for computer forensic training for consideration. The resolution prompted a lively discussion with a dichotomy of opinion. The resolution proposes minimum standards in training based on the RCMP understudy program, which is operated in conjunction with the Canadian Police College. The resolution proposes a minimum of core computer forensic courses as well as the acquisition of 2 additional industry recognized certifications. Members expressed concerns that these training requirements would not be obtainable by the smaller departments due to cost and lack of funding. Members also indicated that it was difficult to send members to CPC for French-only training as a full compliment is required to run a class and therefore those courses are not offered very often.

The discussion on training standards also led to equally lively discussions on the certification and accreditation of computer forensic labs. Members had concerns that the accreditation would create unreachable standards for small and large departments alike and many would be out of the business of computer forensics. Some of the concerns voiced included:

The retention of human resources after a significant investment of time and finances

Cost of equipment to meet standards

Selected persons fail after investment

Rotation of employees through sections, in particular those involved with the viewing of Child pornography

Need for different levels of certification, basic, advanced, optimum

Difficulty to meet constantly changing needs in the area of technology

Anticipation of increase in workload of accredited agencies as a result of download from unaccredited agencies

Creates unrealistic goals that some departments cannot hope to achieve due to human resource and financial limitations as there are problems being experienced presently.

It was agreed that further discussions would have to be conducted on the topic of accreditation of labs at future meetings. It is expected that all members could agree on proposals of minimum training and accreditation if affected departments were properly funded and resourced.

### **Action item 3:**

POWNALL to create new draft of resolution in regards to minimum standards of training.



## **7. Resolution on Blocking IP addresses - Phishing/Spam**

Ray ARCHER has been creating a draft resolution on the blocking of rogue Internet Protocol addresses in relation to Phishing/SPAM and child pornography distribution and communication. ARCHER presented the committee with an introduction to Phishing and SPAM including a report from the Anti-Phishing Working Group as well as informative videos from Microsoft that could be used for public education purposes. ARCHER advised that there are a number of issues that have to be addressed in this resolution including:

Identification of rogue IP address

Identification of rogue IP address that is aligned with legitimate entity

Who determines what constitutes a rogue IP address

Who determines what is Child Porn

Which agency should take action

Protection of ISP's

Ownership of legislation i.e.: CRTC or Criminal Code

Enforcement of legislation

Ease of targets to switch IP addresses within hours to evade detection

### **Action item 4:**

ARCHER to create draft of resolution in regards to the blocking of rogue IP addresses.

## **8. Society for Policing Cyberspace**

Bessie PANG provided members with an overview of a very successful conference that was held in the People's Republic of China. PANG reported on two of the Summit action items:

Computer forensic training needs for PRC prosecutors (especially regarding application of digital evidence) and for PRC police,

Request from PRC prosecutors to POLCYB to arrange for their delegation to visit the Canadian justice system. Their interests are: e-crime legislation and training. POLCYB is looking at inviting them for this fall to Ottawa and Toronto. POLCYB is looking for other interested parties in law enforcement and DOJ to share their experiences with the delegation. PANG also mentioned the Council of Europe's participation at the Summit in China. Margaret Killerby (Head of Dept. of Criminal Problems, COE) presented.

The POLCYB Board has been asked to identify someone from law enforcement in POLCYB to replace Earl Moulton. Stuart Hyde of the West Yorkshire police (UK) is the new president. PANG also provided the Summary of the delegates' recommendations for POLCYB initiatives during round-table discussions on the last day of the Summit. The Board is focusing on the 2 action items as discussed above. PANG will be providing the proposed framework of the concept of establishing a "Cyber-Pol". This was discussed at the round-table discussions and was very well-received. The concept is based on the US Secret Service E-Crime Task Force. Two POLCYB Executives, Tom Musselwhite (USSS) and

Bill Boni (Motorola) will be working further to expand this CyberPol concept for POLCYB. PANG would appreciate feedback on these submissions.

**Action item 5:**

STINNISSSEN to disseminate materials for PANG to committee members

## **9. Informational Items - Roundtable**

Discussion on e-Crime committee input into CACP Strategic planning meeting in January in Winnipeg which will be presented by SMITH to the CACP board. A. SMITH and MacRURY provided comments in regards to the private industries attempts to recover costs for assisting law enforcement for judicially authorized search warrants. A. SMITH and MacRURY are suspicious that costs are would be excessive and private industry would make a profit at the expense of investigations. STINNISSSEN also indicated that e-Crime threads through all criminal investigations and should be recognized as such.

K. SMITH indicated that a new letter would be drafted to CIRA as it appears the original was never received by CIRA.

BENT provided a handout on the functionality of RECOL

**Action item 6:**

BENT to lead discussion on RECOL at the next meeting

## **10. Discussion on Strategic Plan/Next Steps/Annual Report**

Preparation of Annual Report including profile and member updates

**Action item 7:**

ALL members to contact STINNISSSEN and provide bios and update of contact information where necessary.

**Action item 8:**

POWNALL to provide a Representative from the office of Public Safety and Emergency Preparedness Canada – Critical Infrastructure Protection

EISEN to provide a representative from Microsoft re: impact of products (meeting in Spring)

**Action item 9:**

SANSOM to provide article on security on wireless devices from the G8

## **11. Future meetings**

E-Crime Committee Spring meeting will be held on Thursday, May 25, 2006 in Edmonton hosted by David KOROL.

**ACTION item 10:**

ALL members to contact STINNISSEN to determine numbers that will be attending Edmonton

CACP annual meeting St. John's Newfoundland – August 20 –24, 2006.

E-Crime committee meeting to be on Saturday, August 19, 2006 to prepare Chair for committee submissions to CACP Board on August 20, 2006

## Appendix "C"

### Minutes of E-Crime Committee Meeting CACP e-Crime Committee May 25, 2006 Edmonton Police Service

<u>Members participating</u>	<u>Organization</u>
Ken SMITH (Chair)	OPP
Dick BENT	RCMP
Paul ROY	Ottawa Police
Tom POWNALL	RCMP
David KOROL	Edmonton Police
Réal LAGUË	Sûreté du Québec
Alain DUBUC	Sûreté du Québec
Stephan DENIS	Canadian Police College
Ray ARCHER	Canadian Bankers Association
Arni STINNISSSEN	OPP
Bessie PANG	Society for Policing Cyberspace (by phone)
Regrets	
Mike EISEN	Microsoft
Sush GUPTA	Justice Canada
Steve IZZET	Toronto Police
Dan MACRURY	Public Prosecution, Nova Scotia
Gareth SANSOM	Justice Canada
Alex SMITH	Attorney-General, Ontario

#### 1. Opening Remarks

Introductions – The Committee Chair recognized the hospitality of our congenial host, Edmonton Police Service. KOROL provided information on housekeeping items and information.

#### 2. Review of Membership

Dan MACRURY was not present to provide further information on the law enforcement representative from the east coast who is interested in joining the committee. There have been some organizational changes within the Bank of Montreal as a result; someone to replace Ruth Sutton has not been identified as yet. Item to be updated as needed.

***NEW ACTION ITEM 1: East Coast Representative***

**3. Review of Previous Minutes**

Acceptance of minutes (January - Smith)  
Call for additional agenda items

STINNISSSEN to provide committee with information on issues and trends that he has provided in report form to the Federal Provincial Territorial Working Group on Cyber Crime.

Cyberbullying

Wireless (NCECC to be canvassed on an opinion of wireless networks in regards to child exploitation issues, case law, and concerns)

Encryption

Protection of LE tools

ROY advised committee that he is involved with the working group that will be reviewing training as part of the Ontario Association of Chiefs of Police provincial strategy against child exploitation.

POWNALL to provide information to committee on the BOTNET project.

LAGUE to draft letter to CPC regarding the training needs of French speaking officers and the need to satisfy training demands for them. This is as a follow-up to the resolution on Training that will be submitted by this committee.

***NEW ACTION ITEM 2: LAGUE letter***

SMITH advises that the committee has received correspondence that gives the budget approval of \$5,000 for meetings to assist attendance for non-govt and technical advisors that have no travel budget.

**4. Review of Previous Action Items**

**Action item 1:**

STINNISSSEN to determine representative from BMO replacing Ruth Sutton  
Maintain communications with BMO top technical lead went to CIBC – ongoing

**Action item 2:**

MacRURY to draft resolution in regards to amendments to the Criminal Code asking for minimum sentencing for Child Luring offences. *COMPLETED*

**Action item 3:**

POWNALL to create new draft of resolution in regards to minimum standards of training.  
Follow-up- Denis to contact ecole nationale de police du Quebec (ENPQ) for partnership

**NEW ACTION ITEM 3: DENIS**

**Action item 4:**

ARCHER to create draft of resolution in regards to the blocking of rogue IP addresses.  
ARCHER provided the committee with a presentation on what he has accomplished.

**NEW ACTION ITEM 4: ARCHER to provide report for minutes (details in section 7)**

**Action item 5:**

STINNISSSEN to disseminate materials for PANG to committee members.  
*COMPLETED*

**Action item 6:**

BENT to lead discussion on RECOL at the next meeting  
BENT provided the committee with an update on RECOL which is an online Reporting Economic Crime system. It is a system which accepts reports of fraud and filters by keywords, locations, MO and other factors. The system creates a rating for the report and then forwards to the appropriate police agency for further action. RECOL does not deal with the same issues as this committee as it just deals with economic crime rather than e-Crime.  
*COMPLETED*

**Action item 7:**

ALL members to contact STINNISSSEN and provide bios and update of contact information where necessary, especially since the creation of the annual report is underway.  
*ONGOING*

**Action item 8:**

POWNALL to provide a Representative from the office of Public Safety and Emergency Preparedness Canada – Critical Infrastructure Protection. Unable to comply, hopefully for Annual Meeting

**NEW ACTION ITEM 5: POWNALL to continue to canvass PSEPC**

EISEN to provide a representative from Microsoft re: impact of products. Speaker at the Annual Meeting will be the National Technology Officer Michael Weigelt. *COMPLETED*

**Action item 9:**

SANSOM to provide article on security on wireless devices from the G8.  
*ONGOING*

**ACTION item 10:**

ALL members to contact STINNISSSEN to determine numbers that will be attending Edmonton  
*COMPLETED*

## 5. Guest Speaker Centre of Excellence for Canada for High Tech Crime

### **Guest Speaker – Ian Wilms, Centre of Excellence for High Tech Crime in Canada**

WILMS provided committee members with his thoughts and views about the feasibility to create a Canadian Centre of Excellence for High Tech Crime. WILMS used as a reference point the valiant efforts of the many police services across Canada who investigate high tech financial crimes, such as identity theft and credit card fraud as examples. WILMS noted that there was no national coordinated effort and that today's criminal are highly advanced and quickly exceed the capacity and capabilities of Canada's Police. WILMS uses the example of the Australian High Tech Crime Centre that could be emulated. The AHTCC is staffed by members of the Australian Federal Police and State and Territory police from throughout Australia, as well as representatives from private industry and government departments.

The role of the AHTCC is to:

Provide a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions

Assist in improving the capacity of all jurisdictions to deal with high tech crime

Support efforts to protect the National Information Infrastructure.

WILMS appreciated all the candid remarks from committee members who agreed in principle with his ideas while continuing support for local law enforcement as well as staffing the National Centre.

WILMS promised to keep in touch and share developments in the future.

***NEW ACTION ITEM 6: STINNISSSEN to place on Agenda at Annual Meeting for further discussion and action.***

## 6. Guest Speaker – John Evans, Canadian Police Research Centre

*Internet Safety game for school students.*

CPRC was previously involved in an extremely successful computer game designed to be played in schools to teach children Internet safety and how to avoid on-line sexual predators. This game, "MISSING" was (based on a real incident in Vancouver) developed by Livewires [www.livewwwires.com](http://www.livewwwires.com) of Vancouver in concert with police in that area. It has been adopted by several countries to rave reviews and has numerous documented cases where children were in the process of arranging meetings with sexual predators when they played the game and contacted police for help.

There is a new series of games now being completed and released. ("Mirror Image", "Air Dogs", and a third nearing completion). (Based on real incidents, Mirror Image - St. John NB, Air Dogs - Montreal) These will be ready for the coming school year with an estimated world-wide audience of over 38 million students. Although funding has not been raised for distribution in Canada other than Ontario, they are planning release for the fall and hope that enough funding sources pull through. Further contacts would be appreciated).

The University of Lethbridge is going to host video conference train-the-trainer courses throughout the upcoming year for police and teachers. Plans are to start with Alberta officers this summer as our test subjects. Support, promotion and involvement in these valuable programs are appreciated.

#### *LACE - Law against Child Exploitation*

CPRC has worked with a company Blue Bear International ( [www.bbninternational.com](http://www.bbninternational.com)) in the development of a distributed mug shot facial recognition program (<http://www.cprc.org/tr/tr-2004-01.pdf>). This is operational in Chatham-Kent, York and Windsor. This system continues to be developed with a wide variety of modules being made available including auto-aging, 3D modeling (to turn angled facial pictures into the camera permitting auto recognition programs to work), auto facial extraction from video, etc.

Computer crime investigators in York began looking at adapting it to assist them in child porn investigations. York and Blue Bear have since worked to develop it for such investigations. Initial testing by York investigators on real cases has produced very positive results by being able to eliminate more duplicates, reduce manual viewing to a fraction of the time required, do facial capturing in video, and more. In addition, the facial recognition ability to a distributed database network means faces of culprits and victims in the porn can automatically be searched against internal records of other cases, records from other police units, mug shot databases, missing child databases, etc. This offers the potential to build a national or international network to link files and search for the identity of culprits and victims portrayed in the images. The same can also be done for backgrounds.

CPRC demo'd this system to several European police agencies recently and most are very keen to use it and begin linking internationally. York Police have just begun an official trial of the LACE system. CPRC is looking for other police services that would be interested in joining with them to test the networking concept of this system.

#### *CPRC Rebuilding*

CPRC has a business plan before the government calling for a very significant funding increase and the ability to re-organize our structure in order to be more responsive and accountable to the end user (the police community). This business plan was approved by the CACP and the CPPA. While we still don't know when the final decision will be made we have received very positive feedback and the delay provides some time to refine the plan.

Two main thrusts of the plan call for a headquarters (including substantial lab space) to be located in Regina. This center would work very closely with established centers there including the university, police college, RCMP Depot, RCMP Crime Lab, and other industry partners. One of these partnerships is a proposal IT Security Centre of Excellence in cooperation with the U of Regina and various private sector members.

CPRC is committed to being user driven. The second part would be a network of regional managers spread across the country. These regional managers would be responsible for close cooperation between



CPRC and local agencies. These contacts could possibly be embedded within organizations and may even be term secondments vs. static positions. They would be responsible for coordinating involvement in projects within the region and ensuring that issues and priorities from there are represented at the national level.

CPRC is requesting the CACP e-Crime Committee provide CPRC with direction on the following issues;

- A) We need feedback and direction on e-Crime issues and their priorities that we should be consider when selecting R&D projects and funding for them. What is the best means to ensure good communications on such matters between this committee and CPRC?
- B) Should our funding request for a Regina lab facility come to fruition, what facilities and equipment should we consider for this area of R&D? Does the committee or any of its members care to provide input on such a center and its manner of operation?
- C) Would this committee be prepared to offer a letter of support for the re-organization and expansion of CPRC and its funding?

EVANS appreciated the comments from committee members. EVANS promised to keep in touch and share developments in the future.

***NEW ACTION ITEM 7: STINNISSSEN to place on Agenda at Annual Meeting for further discussion and action. A short summary of the business plan to be forwarded to committee members.***

## **7. Discussion on Resolutions**

Resolutions on Training and Request for Minimum Sentencing for Luring discussed and some final amendments made prior to submission. ARCHER recommended to the committee that the resolution proposal for blocking rogue IP addresses should be withdrawn at least for the time being. As a result of his research, there are many hurdles to overcome. There was discussion on other solutions including of voluntary blocking by ISP's. ISP's could amend terms of service which would allow them to legally block rogue IP numbers.

***NEW ACTION ITEM 8: STINNISSSEN to finalize documents for submission to CACP on behalf of the Committee.***

***NEW ACTION ITEM 4: ARCHER to provide written recommendation for Annual Meeting.***

***NEW ACTION ITEM 9: ARCHER to provide article on PHISHING for publication by CACP as an educational piece in their communication documents. The article is largely based on information provided by Microsoft on their website.***

***NEW ACTION ITEM 10: ARCHER to explore possibility of having a speaker from CIOTTA at a future meeting. CIOTTA provides a service that blocks IP's for a fee***

## **8. Informational Items**

POWNALL provided a presentation and proposal on BOTNET.

### ***BOTNET (roBOT NETwork)***

Also called a "zombie army," a BOTNET is a large number of computers on the internet that have been compromised via a Trojan.

Lists of compromised computers sold to hackers and spammers. Hackers and spammers use the BOTNET's to create Distributed Denial of Service (DDoS) attacks and Spam.

Trojan – a malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. Spam - unsolicited email. BOTNET's are usually used for nefarious purposes and a BOTNET's originator can control the "army" remotely through a Control Server. Control Servers are used to control BOTNET's. Globally, Canada is third in the number of control servers at 580. Distributed Denial of Service (DDoS) - is overloading a web site with requests from so many computers that the site become unusable or shuts down. Real world Example of DDoS type of attack using regular postal service - Imagine you are an important politician with a group that opposes you. This group is spread over the world sending you hate mail, soon your mailbox will overflow and any other letters will just spill onto the street and blow away. If you rely on the mail for donations from supporters these will be either lost or stuck amongst the throng of hate mail that you will have to sift through to find. If you receive more mail than you can physically process in a day, some letters will be lost or ignored. Without a foolproof way of detecting donations from the copious hate mail you stand the chance of losing most of your donations and thus are under a DDoS attack on your mailbox. The same kind of thing happens with an internet DDoS Attack – your inbox is so overloaded you will be unable to weed out the good emails from the unsolicited (spam) emails.

- TCB recently took part in int'l BOTNET conference in France
- Tools to assist in BOTNET investigations are being developed by Microsoft
- The RCMP is formulating a strategy to deal with the investigation of BOTNET's
- There are not currently a lot of investigations into BOTNET's being conducted.

The RCMP Tech Crime Program welcomes the input of CACP E-Crime Committee to develop a national BOTNET strategy

***NEW ACTION ITEM 11: To be placed on Agenda at Annual Meeting for further discussion and action.***

### **VOIP Issues**

Voice over Internet Protocol was briefly discussed and it was agreed that this was topic that required further dialogue.

***NEW ACTION ITEM 12: Speaker to be determined for a future meeting (Lawful Access subcommittee)***

### **Update from the Society for Policing Cyberspace**

PANG advised by phone that POLCYB is holding quarterly meetings locally in Vancouver where police and other members are sharing info on what's going on. POLCYB is also collaborating with Simon Fraser University. PANG advised that she has also been involved with the CPRC (John EVANS who coincidentally did a presentation on the same issue) regarding a center of excellence which will gathering info on trends and issues, facilitate information sharing including research amongst our international partners and with local partners. On Oct 23-25, 2006 in Richmond, BC., the international POLCYB

conference will take place and the keynote speaker is from council of Europe Marg Killerby. The conference will promote international collaboration, training, and management of hi tech offenders.

### **Emerging Issues**

STINNISSSEN provided information for the committee members that he believed would be emerging issues for law enforcement and legislation to consider.

#### **Encryption:**

As computers users evolve technology-speaking, security features and improvements are needed to protect themselves and clients from the latest generation of threats including worms, viruses and other malicious software. Recognizing that computer security and the protection of data is a necessity for anyone who goes online, and while more and more users employ encryption, only organizations and individuals with an extraordinary need for secrecy had made use of it. This is beginning to change as the computer industry begins to employ encryption as the normal operating procedure. Illegitimate materials can be and are routinely protected by this form of technology. Encryption software is available free of charge from the Internet or more sophisticated types for purchase. The widespread dissemination of unbreakable encryption without any accommodation for law enforcement access is a serious threat to public safety and to the integrity of Canada's commercial infrastructure.

#### **Wireless Internet Access**

Most access points, when using default settings, are intended to provide wireless access to all who request it. Some argue that those who set up access points without adding security measures are offering their connection, sometimes unintentionally, to the community. Others argue that this reasoning is akin to stating that people who leave their doors unlocked are asking people to take what they like. Using readily available software and hardware in a portable device such as a laptop or Personal Digital Assistant (PDA), a user can simply access an unsecured wireless network. A WI-FI link can be easily found by turning on a wireless receiver and joining a wireless network. Wireless telecommunications is the next major evolution in accessing the Internet with many 'hotspots' or wireless access points being established each day. Consumers including business and private citizens are quick to embrace this new technology without the pre-requisite knowledge as to how secure these networks or that it should even be done. The legalities of accessing an unsecured wireless network is a grey area, one that is creating confusion in the law enforcement community.

#### **Cyberbullying**

Cyberbullying is on the rise as more and more young people connect with the Internet and other forms of technology. Cyberbullying is emerging as one of the more challenging issues facing educators and parents as young people embrace the Internet and other mobile communication technologies. Present legislation is limited and law enforcement is looking for solutions. There is a proposal to make amendments to Section 372, False Messages, of the Criminal Code will assist law enforcement in providing chargeable offences in regards to cyber bullying. At the present time, the Criminal Code provides limited options in cases of cyber bullying, including, criminal harassment, personation and defamatory libel, all of which require specific events/circumstances. Members of the CACP e-Crime committee were canvassed on this sometime ago and all members gave there support.

**NEW ACTION ITEM 13: To be placed on Agenda at Annual Meeting for further discussion and action.**

## **9. Future Meetings**

CACP annual meeting St. John's Newfoundland  
August 20 – 24, 2006

**E-Crime Committee Meeting Saturday, August 19, 2006**

CACP e-Crime Committee Winter Meeting  
Jan 11, 2007 Vancouver