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

Electronic Crime Committee
2014 Annual Report

COMMITTEE MANDATE/OBJECTIVE

"To provide a national leadership role to the Canadian Law Enforcement Community on criminal activity involving technology."

2014 MESSAGE FROM THE CO-CHAIRS

The Co-Chairs are pleased to present the 2013/14 CACP e-Crime Committee Activities Report. We are both new to this role and look forward to working with the committee members to continue being leaders within this fast paced environment. As the pace of internet capable devices increases, so does the impact and implications on law enforcement for evidence gathering. Traditional forensic methods were good enough for the home computer era, but the new mobile capabilities will test our responsiveness in investigation and evidence gathering procedures.

After much discussion and comparison with the definition of cybercrime in various areas of the world, the e-Crime committee has modified its mandate, from ***'e-crime related criminal investigations'*** to ***'criminal use of technology'***. This, it is hoped, will capture all technologically facilitated crimes, including 'pure' cybercrime and cyber-bullying, as examples. To keep with this mandate we have identified a number of priorities the committee will work on in the coming year. We have also provided a synopsis of the accomplishments over the last twelve months.

In the coming year we hope the committee, with the assistance of our National Tech Crime Advisory sub-committee, will make headway on a number of initiatives. Specifically we continue to support the development of a Digital Field Triage Program aiming to train frontline police officers to gather basic digital evidence from search scenes. We also hope to work with the telecoms industry to define mobile device theft mitigating strategies and with public sector partners to identify metrics and statistical data to identify the magnitude of e-Crime events within Canadian society. While continuing to develop a Canadian Law Enforcement (LE) cybercrime strategy we will strive to ensure LE partners share information and avoid duplication of efforts. We will study the impacts of offsite data storage and processing (cloud computing) on Canadian criminal investigations. We will open discussions with various other CACP committees to identify the scope of our mandate and what roles are better suited to the e-Crime committee.

The ubiquity of technology in every facet of society enables criminals to find new and creative ways to conduct illicit activities. The e-Crime committee will work on developing strategies to efficiently combat emerging trends in criminality. We will continue to diligently advocate for ways to enable Canadian LE to have the appropriate tools, both technical and judicial, to protect Canadians from technology enabled crime and prosecute criminals to the full extent of the law. Law Enforcement must be provided the appropriate tools to find the proverbial technological fingerprint left by criminals both online and in the real world.

The committee will position itself to respond to changes brought on by the recent Canadian Supreme Court Spencer ruling. Telecommunication service providers are reacting to the decision and the current way of doing business will change. We look forward to working with

the industry to determine the best way to work within these newly imposed legal constraints, as well as the recent tendency by the industry to charge for certain services. The Law Enforcement community has always believed in privacy for the online community. We have also always advocated for reducing the ability for criminals to be anonymous. It is imperative that law abiding Canadians know that their Law Enforcement officials will be able to gather evidence lawfully, in order to stop criminal activity and bring those responsible before the Courts. With this in mind, we are currently implementing a new system allowing for the efficient interception and collection of lawfully authorized internet traffic from criminals.

The Committee is composed of Canadian police leaders, private sector special advisors, justice experts and technical advisors. The Committee membership includes police representatives from the RCMP, Ontario Provincial Police, Sûreté du Québec, as well as Toronto, Ottawa, Saskatoon and Edmonton Police Services. The private and not for profit sectors are represented by the Canadian Bankers Association, Microsoft Canada and the Society for the Policing of Cyberspace. We aim to increase participation by engaging police at the senior executive level and bringing in partners from academia. We thank all the committee members for their continued engagement as we navigate this high priority environment. Together we will make a difference to reduce victimization of Canadians at the hands of criminals abusing technology to achieve their nefarious intent.

The Committee would like to acknowledge the outstanding contributions of past members: Capitaine Frédérick GAUDREAULT, Co-Chair of the e-Crime Committee (2012-2013) Sûreté du Québec and Superintendent Tony PICKETT, Co-Chair of the e-Crime Committee (2011-2013) RCMP Technical Investigation Services. We wish you well in your future endeavors.

As co-chairs of the e-Crime committee, we look forward to a year filled with challenges that we are confident we will be able to respond to in a productive manner. The committee members will be steadfast in their continued hard work and dedication to protect Canadians from criminals intent on facilitating their crimes by using technology to undertake new and creative illicit activities.

Deputy Commissioner Scott TOD
Ontario Provincial Police

Chief Superintendent Jeff ADAM
Royal Canadian Mounted Police

PROGRESS ON 2013/ 2014 INITIATIVES:

- **The CACP e-Crime Committee will support a Virtual Currencies Project (BitCoin). This multi-stakeholder project will analyze this new form of currency, specifically investigational issues in Canada:** The e-Crime committee supported a research project into the digital currency Bitcoin. The research was conducted by the RCMP Technical Investigation Services (TIS) in parallel with RCMP Federal Policing. The TIS research identified a generic methodology that will allow Forensic Analysts to tackle any Bitcoin related investigation, while the Federal Policing facet looked at services dealing in Bitcoins for potential investigational opportunities. The project is expected to conclude with the results being collated and disseminated within the Canadian Law Enforcement community.

- **The CACP e-Crime Committee will support the development of an EnCase 7 software workshop allowing analysts to transition from previous versions of the computer forensics software:** The Canadian Police College did not complete a workshop for the transition to this new version of the EnCase computer forensic software. The CPC has however transitioned to this new Forensic Software as part of the Computer Forensic course provided as a base course to all Canadian Law Enforcement officers joining a Technological Crime Unit.

- **The e-Crime Committee will support continued work to develop a Digital Forensic Methodology to be used by the Canadian LE community. This initiative continues work initiated in 2012/13:** The e-Crime Committee continues to support the establishment of a Digital Forensic Methodology (DFM). A Subject Matter Expert (SME) working group composed of SMEs from various Canadian LE agencies has been established. The group has completed a high level conceptual model of the DFM aligning with a pre-existing International Standards Organization standard (ISO 27037). The work is continuing with the goal of developing a comprehensive model for use within the Canadian LE community. The DFM content once put in place will allow analysts to have a central reference for best practices in the field of digital forensics.

- **The e-Crime Committee will support the work of a newly created sub-committee (Cybercrime Consultative Group) to examine and share best practices, educational opportunities, investigative information and other facets of cybercrime (pure computer crime):** The Cybercrime Consultative Group was created and met once via teleconference. This initial meeting served as an introduction to the key players involved in operational cybercrime investigations. This initiative however did not carry-on past this initial informal meeting of key players. The E-crime committee will explore different approaches that will provide better tools to examine these issues.

- **The e-Crime Committee will continue to support the development of a National Cybercrime Strategy:** The e-Crime committee continues to support the development of a truly National Cybercrime Strategy. In response to the Cybersecurity Strategy put forward in 2010 by Public Safety Canada, the RCMP has recently developed a draft Cybercrime strategy. In partnership with other Canadian Law Enforcement Agencies, the RCMP wishes to continue to tackle the operational aspects of implementing a strategy to pursue the fight against Cybercrime. The e-Crime Committee is well positioned to lead these efforts to define and tackle Cybercrime at the National Level.

- **The e-Crime Committee will endeavour to form partnerships with Canadian academia, including Canadian universities, who have an interest in providing a safe cyber environment for all Canadians:** The e-Crime committee continues to support increased partnerships with Canadian academia. The SQ has maintained its participation with the National Cyber Forensics Training Alliance (NCFTA) Canada, based at Concordia University in Montreal. The NCFTA's Canada director was invited to join the e-Crimes committee as an Associate Member. The RCMP Technical Operations Branch has initiated a promising partnership with the Royal Military College of Canada. The Calgary Police Service has initiated a partnership with the University of Calgary in an effort to improve the collective response to cybercrime and cybersecurity. The OPP has initiated a relationship with the University of Ontario Institute of Technology (UOIT). Both groups have been working cooperatively to identify research projects which are of mutual interest and to benefit from knowledge sharing. Various CACP represented agencies are also participating in Serene-Risk (Smart Cyber Security Network). This is a cooperative between government agencies, police, private sector and academia with an aim to make Canada the most secure cyber network in the world. This group is in the initial stages of development and has excellent representation from a broad cross-section of National partners.

INITIATIVES PLANNED FOR 2014/ 2015:

- **The e-Crime Committee will continue to support the development of a National Digital Field Triage Program.**

- **The e-Crime committee will explore the implications of the proposed "kill Switch" initiative proposed by telecommunications providers and engage with industry partners to determine the best way forward.**

- **The e-Crime committee will research the current status of statistical data being gathered to identify various types of criminal activity facilitated by technology, explore best practices and ensure appropriate metrics are collected.**

- **The e-Crime committee will explore the impact of Cloud Computing on criminal investigations by determining what facets negatively impact investigations and engaging with various stakeholders to determine mitigating initiatives.**

- **The e-Crime committee will promote the development of a CACP lead cybercrime fighting strategy.**

- **The e-Crime committee will lead a project to ensure e-Crime investigations carried out by Canadian Law Enforcement Agencies are de-conflicted to avoid duplication of efforts.**

- **The e-Crime committee will engage with the Law Amendments Committee to discuss the scope of the Lawful Access and Electronic Surveillance (LAES) sub-committee and whether its mandate better fits within the e-Crime committee's purview.**

DATES/OVERVIEW OF MEETINGS

The e-Crime Committee meets in the fall to identify goals and objectives. Intersessionally, the Committee uses email and teleconferencing to further discuss objectives/initiatives and to determine an appropriate action plan for these items. A spring meeting is held to ensure action items have been addressed. The Committee members who participate in the meetings are supported by their respective organizations. CACP Board of Directors provides funds to offset certain expenses such as conference rooms and other logistical requirements.

Fall 2013
NTCAC & CACP E-Crime Committee Meeting
October 2nd – 4th, 2013
Toronto, Ontario

The fall meeting of the CACP e-Crime committee and of the National Tech Crime Advisory Committee (NTCAC) was held in Toronto. The below points outline the topics discussed during these 3 days:

- Introduction of committee members and overview of the current status of each of the participants units.
- Discussion on current Case Law with respect to Search Warrants and Court Procedures.
- Discussion on the trans-border access to data.
- Discussion held on the current statistical collection of data pertaining to cybercrime investigations.
- Discussion on the impact of Corporate IT involvement with the Tech Crime Units
- General discussion on the use of Civilian Members vs Police Officers.
- Presentation of a large child exploitation case by the O.P.P.
- Discussion on certification pre-requisites at the Canadian Police College.
- Presentation on the National Cyber-Forensics and Training Alliance Canada by Dr. Mourad DEBBABI.
- Presentation on the International Cyber Security and Policing Conference co-hosted by POLCYB (The Society for the Policing of Cyberspace) by Ms. Bessie PANG.
- Presentation on the Microsoft Digital Crimes Unit by Mr. John WEIGELT.
- Update provided by the co-chairs and discussion on new initiatives for 2013-2014.

Spring 2014
NTCAC & CACP E-Crime Committee Meeting
May 7th – 9th, 2014
Calgary, Alberta

The spring meeting of the CACP e-Crime committee and of the National Tech Crime Advisory Committee (NTCAC) was held at the Calgary Police Service (CPS) Headquarters and hosted by CPS. The below points outline the topics discussed during these 3 days:

- Introduction of all attendees and election of new Chair of the NTCAC.
- Discussion on serving assistance orders and production orders on various IT industry companies.
- Discussion on use of major computer forensic software and mobile device analysis hardware and software within various LE units.
- Discussion of categorization of Child Exploitation images and tools used.
- Update on Digital Forensic Methodology project and upcoming steps discussed.
- Discussion on the cellphone kill switch project advanced by the Canadian Wireless Telecommunications Association (CWTA).
- Presentation by Mr. Angus MACDONALD of Trend Micro with respect to increased partnership with Canadian Law Enforcement.
- Presentation and discussion on the Digital Field Triage project.
- Presentation on the RCMP Cybercrime Strategy.
- Discussion on the capture of statistical data on Cybercrime investigations.
- Update provided on Tech Crime Learning Institute at the Canadian Police college.
- Update provided on the Society for the Policing of Cyberspace (POLCYB) by Ms. Bessie PANG.
- Presentation on the anatomy of a retail breach by Mr. Ray ARCHER.
- Presentation on a Heartbleed investigation.
- Update provided on Jurisdictional issues by Mr. Gareth SANSOM of Justice Canada.
- Update provided as to status of Bill C-13.
- Discussion on various administrative issues relating to the e-Crime committee (Terms of Reference, election of Chairs, composition,….).

The e-Crime committee also held two teleconferences. The meetings were held in the spring and summer of 2014. The teleconferences served to finalize agenda items, discuss initiatives and solicit information for the completion of the yearly report.

Activities Planned/Significant Dates 2014/2015:

Aug 24th – 27th, 2014	Submission of 2014 Annual Report Annual CACP meeting Victoria, British Columbia
Oct 16th – 17th, 2014	Committee Meeting Ottawa, Ontario
Winter 2014	Committee Teleconference (approx. February)
Spring 2015	Committee Meeting (Location TBD)
Summer 2015	Annual CACP Meeting - TBD
Fall 2015	Committee Meeting (Location TBD)

CACP E-CRIME COMMITTEE MEMBERS LIST:

CACP Members

D/Commr Scott TOD (Co-Chair)	Ontario Provincial Police
C/Supt Jeff ADAM (Co-Chair)	RCMP Technical Investigation Services
Supt Maury MEDJUCK	RCMP Technical Investigation Services
André BOILEAU	Sûreté du Québec
Thomas FITZGERALD	Toronto Police Service
Grant FOSTER	Saskatoon Police Service

CACP Associate members

Ray ARCHER	Canadian Bankers Association
Bessie PANG	Society for the Policing of Cyberspace (Polcyb)
John WEIGELT	Microsoft Canada

Technical Advisors

Dan MacRURY	Nova Scotia Public Prosecution Service
Carole MATTHEWS (Secretary NTCAC)	Ontario Provincial Police
Phil PALAMATTAM (Chair NTCAC)	Calgary Police Service
Maurizio ROSA (Secretary E-Crime)	RCMP Technical Investigative Services
Gareth SANSOM	Justice Canada
France THIBODEAU	Canadian Police College

Success Stories 2014

In 2013 the Calgary Police Service established a Cybercrime Support Team. This team provides assistance to other areas of the Service with online/internet investigations, covert operations and intelligence gathering. The team supported 205 requests for assistance in 2013 including a wide variety of investigations such as homicides, electronic theft and fraud, criminal harassment, robbery, missing persons and organized crime. The Cybercrime team is projecting 350+ requests for assistance in 2014.

One example of the excellent work they do was their response to a public safety threat. In early June 2013, the Calgary Fire Department received and email threatening the safety of the public at the Calgary Stampede. The email read "There is going to be a machine gun attack at the Stampede this year. Two MG-53's at 1800rpm. There will be over 1000+ casualties. These machine guns can fire over 1000 rounds before malfunction." The Calgary Police Service Cybercrime Support Team was brought in to the investigation. Working with partners in the cybercrime community, the team sourced the email back to a person of interest. It was learned that this individual had a history of mental health related issues and was known to be in possession of firearms.

A search warrant was executed at the person's residence where investigators recovered a Glock 9mm handgun, multiple high-capacity magazines, an AR-15 rifle, an Enfield rifle, hundreds of rounds of ammunition and a number of computers. Forensic analysis of the computers conducted by the Calgary Police Service Technological Crimes Team revealed multiple documents related to terrorism. The person was charged with 25 Criminal Code charges and underwent a psychiatric assessment.

The Cybercrime and Tech Crimes teams have partnered with the University of Calgary Department of Computer Science and the Institute for Security, Privacy and Information Assurance to combine expertise in an effort to improve our collective response to cybercrime and cybersecurity. They have also reached out to private industry to identify opportunities to work together on improving forensic capabilities and developing cybercrime initiatives.

The Saskatchewan Internet Child Exploitation Unit was involved in a multi-agency Canada wide investigative project-Operation Snapshot III. The operation was coordinated by the National Child Exploitation Coordination Centre (NCECC), a division of the Canadian Police Centre for Missing and Exploited Children/Behavioural Sciences Branch (CPCMEC/BSB) in Ottawa. Project SNAPSHOT III, which ran from February 1 to May 27, 2014, involved ICE investigative Units from across Canada. This proactive project focused on individuals utilizing file sharing networks where child sexual abuse media is disseminated, as well as any other networks where child exploitation occurs. During SNAPSHOT III, the Saskatchewan ICE Unit initiated 15 investigations and executed 13 search warrants throughout the Province, and 35 Criminal Code charges were laid. Twelve persons were charged.

The Saskatchewan ICE Unit executed a search warrant in Springside, Saskatchewan in December 2012. At that time a male was charged with Possession of Child Pornography. Through categorizing the seized images, the ICE investigator located videos of the suspect sexually assaulting a young girl approximately five years old. The ICE investigator was eventually able to determine the identity of the young child and that the offences took place in Doha, Qatar, while the suspect was working overseas. The victim and family were now residing in Thailand. In consultation with Saskatchewan prosecution and the use of section 7(4.1) of the Criminal Code, the Saskatchewan ICE Unit sent a three person team to Bangkok, Thailand in August 2013. With the assistance of the Royal Thai Police, Interpreters, and victim support personnel, the ICE members were able to obtain statements from the victim and family members to lay additional charges back in Canada. The suspect was charged and pleaded guilty prior to court.

In February, 2014, members of the Saskatchewan ICE Unit were called to assist RCMP members in Yorkton, Sk., regarding a possible Obstructing Justice investigation. In August, 2013, a Saltcoats, SK resident was charged with Sexual Interference and Invitation to Sexual Touching on a 14 year old female victim. The accused was released on conditions of no contact with the child victim. In January, 2014, the female victim began getting messages from an u/k male through social media sites. This u/k male befriended the victim and in time began trying to persuade her to drop the charges against the male that assaulted her, because he is a good person. ICE members took over the child's account profile. Through the chats, this u/k male began to leave the victim gifts buried in the ground near her school. RCMP members and ICE Unit members observed the original offender at these drop sites. A search warrant was drafted and the original accused offender was arrested again and charged with Obstructing Justice, Intimidation of a Justice System Participant, Invitation to Sexual Touching, Sexual Interference, Child Luring, and Breach of Undertaking x 7.

In November 2011 Ontario Provincial Police investigated the violent murder of a Brampton, Ontario realtor by his tenant and an associate of the tenant. Both were charged with first degree murder. A large number of computers, storage devices and mobile phones seized during the investigation from the accused and victim, were submitted for examination by the OPP Technological Crime Unit (TCU). Assistance of the OPP TCU met with success on a number fronts during this investigation.

· Prior to the analysis of the exhibits, the original search warrant was reviewed and deficiencies were noted. Recommendations were forwarded from the OPP TCU to the investigative team, who redrafted search warrants twice, before the examination of the exhibits proceeded. Although the search warrant issue was strongly contested during pre-trial motions, it is believed that the diligence and good faith demonstrated during the course of this process was respected by the trier of fact and his critical in his decision to allow all the evidence. This has served to validate procedures in place at OPP TCU, which ensure quality warrants have been endorsed prior to exhibits being examined.

· Remote access to the data was configured so that an investigator could review a variety of potentially relevant subsets of data extracted from the submitted exhibits from his home location. The original evidence and results of the data review were maintained secure at the OPP TCU and additional software licensing was not required to be purchased. Results were compiled back at the OPP TCU, for purposes of disclosure as well as additional validation and analysis.

· Several locked mobile devices were sent to the RCMP Technical Analysis Team (TAT) in Ottawa, who were successful in extracting and returning data to these devices for additional processing and analysis.

· The exhibits were processed using a very cooperative team effort, with both police officers and civilian members of the OPP TCU completing the imaging, pre-processing and analysis of the data.

· The examination of mobile devices yielded highly relevant findings, located by virtue of a high degree of knowledge and ability, as well as persistence in trying newly developed software against the data, over the course of the years that this data was available for that purpose.

· The Crown Attorney who prosecuted the case was highly complementary in his praise of the caliber of testimony provided during the trial, by both of the civilian members who completed the analysis of the computers and mobile devices.

The two accused have been found guilty of first-degree murder and sentenced to life in prison.

In October 2013 Omegal (social networking site which is a spin-off of chat roulette) contacted Barrie Police ICE via, NECMEC and the RCMP NCECC. An upload of a movie showing the sexual exploitation of a baby was reviewed. Through the help of Omegal they flagged the suspects IP and sent a cookie to his computer so it could be identified by police.

The investigation commenced and a search warrant was conducted on a residence in Barrie. As a result of the search, a male was arrested who turned out to be the father of three children in the home. All three appear to be victims after the computer was analyzed.

The police forensic unit initially examined a laptop and an iPad and a iPhone, with no results to support the charges. The suspect was adamant that he was a stay at home dad who never really touched computers and didn't have a phone. He was arrested due to the fact that he was identified on the video through an exact match of a shirt he was wearing, which had very identifiable markers printed on it.

After the arrest investigators conducted an extensive search of the residence as they knew the suspect must have hid a computer in the house. After an hour of searching D/C Pinkerton using his height to his advantage was able to look behind a very large 60 " projection TV in the basement den. Down the back of the TV and purposely hidden by the accused was the brand new laptop.

By examining that laptop on scene, forensic examiners were able to find evidence that the suspect had downloaded images of child pornography. Further to that an old analog Motorola cell phone was located and seized. Through analysis of the micro SD card several new movies of the accused sexually assaulting his children were found in unallocated space after he had deleted the material.

The accused is the children's biological father and has been in custody since November 2013. He is currently working out a guilty plea with the Crown for which the Crown is seeking a 15 year sentence.

Other information also revealed links to the UK which are being investigated.

In May 2014, the RCMP Integrated Tech Crime Unit (ITCU) in C Division (province of Quebec) participated in an operation of international scope. The investigation initiated by the Federal Bureau of Investigation (FBI) and coordinated by Eurojust, targeted computer hackers using malware allowing them to create several botnet networks. Botnets being networks composed of infected computers remotely controlled by the hackers. On May 13th and 14th significant take-downs were simultaneously conducted in approximately 15 countries. Over 300 searches and 81 arrests were carried-out. In order to limit the number of victims, ITCU investigators from C Division carried out searches in 15 separate locations throughout the province. All of the seized evidence is currently being analyzed by the ITCU investigators.
