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
2015 Annual Report

COMMITTEE MANDATE/OBJECTIVE

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

2015 MESSAGE FROM THE CO-CHAIRS

The CACP Electronic Crime (e-Crime) Committee Co-Chairs are pleased to present the 2014/15 yearly report on activities. Having taken on the leadership of this committee a year ago, we are happy to take stock of the accomplishments made by the membership. The fast moving pace of innovation in the telecommunication and information technology sphere is at times astounding. Having subject matter experts available to properly counsel and advise us is critical.

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, Montreal, Vancouver, Ottawa, 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. These members, along with the members making up the National Tech Crime Advisory sub-committee (NTCAC) and the recently added Lawfully Authorized Electronic Surveillance sub-committee (LAES), provide us with the ability to keep our finger on the pulse of this ever changing environment.

The coming into force of Bill C-13 has provided some long sought after solutions for Law Enforcement agencies to deal with various types of criminality not previously specifically addressed. A new set of judicial orders are now available to investigators to allow them to obtain information lawfully in order to identify criminals and stop them from victimizing innocent Canadians. In consultation with various stake holders and partners both nationally and oversees, committee members strive to adapt to these changes in order to meet the committee's goal of providing a national leadership role to the Canadian Law Enforcement Community on criminal activity involving technology.

This year, the e-Crime committee took on the responsibility of the Lawfully Authorized Electronic Surveillance sub-committee. Through their continued hard work in the area of lawful interception of telecommunications, members of the LAES provide the e-Crime committee with advice on changes and initiatives required to promote the efficient use of technical means to gather critical evidence in the most serious of criminal activities. We are looking forward to advancing initiatives proposed by the LAES sub-committee and specifically to respond to changes brought on by the recent Canadian Supreme Court Spencer ruling.

The National Tech Crime Advisory Committee, composed of senior members leading digital forensics and cybercrime units of Canadian Law Enforcement Agencies, continued to work toward achieving initiatives identified by the e-Crime committee. The NTCAC strives to improve the overall capabilities of Cyber and Tech Crime Units, investigating offences and preventing duplication of efforts. The NTCAC chair persons attended our spring meeting and presented on various issues. We continue to be grateful for their dedication and sound advice.

Law-abiding Canadians continue to be targeted by various online extortion schemes. In several cases Canadian victims have seen their computer data encrypted in an attempt to have them pay a “ransom” to obtain a decryption code. The continued flood of bad news regarding compromises of various governmental, medical and corporate networks slowly frays public confidence in the use of online tools. The continued migration towards remote storage and tools (use of “the cloud”) is another dimension that criminals can exploit to their benefit. Law enforcement continues to struggle with carrying out investigations which will lead to identifying these threat actors. The increasing ability for criminals to anonymize themselves prior to engaging in their illicit activities is hindering the timely actions of Law Enforcement. The international nature of cyberspace, as everyone can comprehend, also complicates the work of our investigators. Criminals are savvy in their ability to pick the right nation state from which to carry out their attacks. It is ever more evident that a joint approach to this problem is necessary. Models involving partnerships between private enterprise and public institutions are key in achieving this goal.

The CACP heads into 2016 with cybercrime as a guiding theme. The CACP has funded a Global Studies Group which met with various stakeholders, in Canada and overseas, in order to properly advise the Chiefs of Police on the best practices to make headway against the scourge of cybercriminals. As we prepare for 2016 and the CACP annual meeting to be held in Ottawa under this cybercrime theme, the e-Crime committee will take note of the recommendations brought forth by the group and endeavor to properly advise the CACP on the best way forward.

Canadians of all stripes rely on their law enforcement community to bring cyber criminals to justice. Police agencies nationwide have recognized that creating cyber units is a sound method of addressing the growing number of complaints received from the public. Law Enforcement in Canada strives to form partnerships with Federal agencies, private industry and foreign entities in order to combat against online criminals. Cyber criminals increasingly target networks with what seems like impunity. We believe the collaborative approach extoled by Canadian Law Enforcement will pay dividends and allow us to make headway in keeping Canadians safe from online actors with nefarious intent.

As co-chairs of the e-Crime committee, we look forward to a challenging year where Cybercrime will be at the forefront of the Canadian Law Enforcement agenda. Alongside the motivated members of our LAES and NTCAC sub-committees, the members of the Electronic Crime committee are confident we will achieve great strides in ensuring Canadians can safely navigate the internet and feel secure in doing business and socializing online.

Deputy Commissioner Scott TOD
Ontario Provincial Police

Chief Superintendent Jeff ADAM
Royal Canadian Mounted Police

PROGRESS ON 2014/ 2015 INITIATIVES:

- **The e-Crime Committee will continue to support the development of a National Digital Field Triage Program:** The e-Crime committee supported the development of a National Digital Field Triage Program aimed at providing frontline investigators with abilities on various digital devices in order to facilitate timely analysis of seized evidence. A successful Digital Field Triage Program is currently in place in the RCMP's E Division (British Columbia). This program has been presented to other Canadian Law Enforcement agencies and interest has been growing. We are currently exploring the best model for delivery to the Canadian Law Enforcement community as a whole.

- **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:** Some information gathering was conducted regarding this potential initiative proposed by telecommunication providers in Canada. To date the issue has not been well framed for presentation to the e-Crime committee in order for decisions/recommendations to be made. As such this initiative is concluded pending a renewed impetus from industry and additional clarity on the issue.

- **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 has determined that in order to better identify issues within the cybercrime realm and gaps within Law Enforcement's approach to the problem, proper metrics need to be collected. To date there has unfortunately been little headway in properly identifying statistical data currently being collected and what additional data should be collected. Discussions will continue with Statistics Canada in order to advance this initiative. The National Technological Crime Advisory Committee (NTCAC - a sub-committee of e-Crime) members are currently spearheading this initiative.

- **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-Crimes committee continues to believe Cloud Computing will affect the future of investigations. Little progress was done on this initiative due to other pressing matters occupying resources dedicated to looking into the issues. This initiative will be brought forward as an initiative for the coming year. The NTCAC will continue to frame the issues and potential impacts in a manner that will allow the e-Crime committee to make sound recommendations going forward.

- **The e-Crime committee will promote the development of a CACP lead cybercrime fighting 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 developed a draft Cybercrime strategy. This strategy was presented to all e-Crimes committee members and an overall CACP strategy will be developed in consultation with other Canadian Law Enforcement Agencies. The e-Crime Committee will continue to tackle the operational aspects of implementing a strategy to pursue the fight against Cybercrime and is well positioned to lead these efforts to define and tackle Cybercrime at the National Level. This initiative will continue in 2015/2016.

- **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:** Some discussions were held with various Federal partners and assessments of existing databases or other means of de-confliction explored. No immediate solution was evident from the reviews that were carried out. This initiative will be brought forward for the new year as part of a broader look into International and domestic de-confliction and coordinated investigations. The committee hopes to leverage the work done this year by the Executive Global Studies cohort.

- **The e-Crime committee will engage with the Law Amendments Committee to discuss the scope of the Lawfully Authorized Electronic Surveillance (LAES) sub-committee and whether its mandate better fits within the e-Crime committee's purview:** The LAES is now a sub-committee of the e-Crimes committee. This initiative is concluded.

INITIATIVES PLANNED FOR 2015/ 2016:

- **The e-Crime committee will advance the Cybercrime theme and lead the preparation for the CACP Annual Conference in Ottawa for 2016.**

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

- **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 broad project while engaging the CACP to ensure e-Crime investigations carried out by Canadian Law Enforcement Agencies are de-conflicted domestically and internationally. We will develop a coordinated approach to investigations with international scope (botnet takedown type of investigations). We will ensure information regarding training/meeting/conference opportunities is shared, and that some oversight is provided to ensure appropriate attendance and value comes from attending. We will leverage the work done this year by the Executive Global Studies cohort.**

- **The e-Crime committee will continue to partner with TELCOs in order to facilitate future dealings to overcome issues resulting from SPENCER decision and increased fees.**

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. The chairs of the LAES and NTCAC sub-committees attend the meetings and report on their endeavours during these meetings. The CACP Board of Directors provides funds to offset certain expenses such as conference rooms and other logistical requirements.

Fall 2014
CACP E-Crime Committee Meeting
October 16th – 17th, 2014
Ottawa, Ontario

The fall meeting of the CACP e-Crime committee was held in Ottawa and hosted by the Ottawa Police Service. The below points outline the topics discussed during these 2 days:

- Introduction of newly appointed committee chairs and roundtable introduction of members attending.
- Discussion on new roles for NTCAC and CACP Committees. Clear definition of NTCAC mandate and expected endeavours and reporting mechanisms.
- Discussion and presentation of initiatives for 2014-2015.
- Discussion of the long term strategic outlook.
- France THOBODEAU provided an update of the Canadian Police College Technical Crime Learning Institute.
- Presentation by Ottawa Police Service investigators of Project Winter.
- Presentation by the Ontario Provincial Police of Project Greenwell/Blackheath.
- Presentation by Gareth SANSOM of Justice Canada on the Supreme Court of Canada SPENCER decision.
- Presentation on POLCYB (The Society for the Policing of Cyberspace) by Ms. Bessie PANG.
- Presentation by Martin GIRARD and Alain MONFETTE of Bell Canada.
- Update provided by the co-chairs and discussion on initiatives for 2014-2015. Identification of action items.
- Discussion of current international partnerships and police activities.

Spring 2015
CACP E-Crime Committee Meeting
May 13th – 14th, 2014
Vancouver, British Columbia

The spring meeting of the CACP e-Crime was hosted by the Vancouver Police Department. The below points outline the topics discussed during these 2 days:

- Introduction of all attendees and presentation of the agenda.
- Presentation by the Chair of the NTCAC sub-committee. Review of the initiatives and discussion on way ahead for 2015.
- Presentation by the Chair of the LAES sub-committee. Review of the initiatives and discussion on way ahead for 2015.
- Update provided on the Society for the Policing of Cyberspace (POLCYB) by Ms. Bessie PANG.
- Presentation on the Smarter Cities concept by Peter MCFADDEN of IBM.
- Presentation by Peter CUTHBERT of the CACP on 2016 CACP annual meeting to be held in Ottawa under the Cybercrime theme.
- Presentation by Supt Bernie MURPHY of the OPP on Serene-risc (Smart Cyber Security Network).
- Re-cap and discussion by Chair on new initiatives for 2015-2016. Identification of action items.

The e-Crime committee also held two teleconferences. The meetings were held in the spring and summer of 2015. The teleconferences served to finalize agenda items, discuss initiatives and solicit information for the completion of the yearly report.

Activities Planned/Significant Dates 2015/2016:

Aug 24th – 27th, 2015	Submission of 2014 Annual Report Annual CACP meeting Victoria, British Columbia
Nov 4th – 5th, 2015	Committee Meeting Quebec City, Quebec
Winter 2015	Committee Teleconference (approx. January)
Spring 2016	Committee Meeting (Location TBD)
Summer 2016	Annual CACP Meeting - Ottawa
Fall 2016	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**
Paul BEESLEY	Ontario Provincial Police
André BOILEAU	Sûreté du Québec
Darren DERKO	Edmonton Police Service
Kathryn MARTIN	Toronto Police Service
Joan McKENNA	Ottawa Police Service
Maury MEDJUCK	RCMP Technical Investigation Services
Ralph PAUW	Vancouver Police Department
Gaétan VAILLANCOURT	Service de Police de la Ville de Montréal

CACP Associate members

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

Technical Advisors

Vern CROWLEY (Secretary NTCAC)	Ontario Provincial Police
Peter HAMMERSCHMIDT	Public Safety Canada
Joel KULMATYCKI (Co-Chair LAES)	Toronto Police Service
John MENARD (Co-Chair NTCAC)	Toronto Police Service
Phil PALAMATTAM (Co-Chair NTCAC)	Edmonton Police Service
Hollie RIORDAN (Co-Chair LAES)	Vancouver Police Department
Maurizio ROSA (Secretary E-Crime)	RCMP Technical Investigative Services
Gareth SANSOM	Justice Canada
France THIBODEAU	Canadian Police College

SUCCESS STORIES 2015

The Integrated National Security Enforcement Team (INSET) unit of the RCMP in C Division (province of Quebec) has increased its reliance on the seizure and analysis of digital devices as the Internet and social media are thought to be prime contributors to the radicalisation of vulnerable youths. These youths are using mobile devices and laptops designed for browsing (Chromebooks) and use the Internet Cloud services for storage. The results of this are twofold: the devices often prove technically new and challenging, and much of the information that investigators are seeking is not on the device but stored in the Cloud in another jurisdiction. This has resulted in an increased workload to the RCMP Integrated Tech Crime Unit (ITCU). INSET is investigating many threats from High Risk Travelers. Another 10 individuals were arrested in May, suspected of wanting to join terrorist groups overseas. This led to a further 117 digital items, including 40 mobile devices, being seized by police which require analysis by the ITCU. This investigation is also on-going.

In April 2015, the support of the Montreal ITCU was requested for a number of searches conducted by the INSET. INSET had conducted an investigation after information was received from the community. The investigation showed that two Montreal area students were planning to leave the country to commit a terrorist act abroad. Seized in the search were 3 computers, 10 mobile devices and 8 other digital devices which were later analyzed by the ITCU. Significant and relevant evidence was located which assisted the investigation.

The result was that the two students, both aged 18, were charged with the following: Attempting to leave Canada to participate in the activities of a terrorist group; Facilitating terrorist activity; Commission of an offence for a terrorist group; Using explosives; The two Montreal residents, who are 18 years old, are currently in preventive detention and the case is before the courts. The investigation is still ongoing. This case came only days after the arrest of two other Montrealers for terrorism related offences that were then released on Peace Bonds. The two suspects were ordered to wear GPS bracelets, allowing the RCMP to track their movements. The suspects also had conditions which restricted their use of computers. The ITCU also assisted in the investigation that lead to the arrest and later assisted in monitoring of the suspects' computer use. Following the monitoring, one of the suspects was arrested for breaching the Peace Bond. His computer was seized and analyzed by the ITCU for evidence to support the charges. The case is still before the court.

Created in 2010, Project Clemenza aimed at dismantling two major Italian organized crime organizations. These networks' main goals were drug trafficking and trade rights within the Montreal area and used several dozen encrypted Blackberry devices for covert communications. C division ITCU with assistance from the RCMP Technical Analysis Team located in Ottawa provided the technical expertise in analysing and managing the various electronic devices seized during the operation. A large number of Blackberry devices were analysed and various techniques were used to decipher the encoded

messages. This allowed a clear view of the methods and procedures used by the various parties involved and allowed charges to be brought against several key figures.

In April 2015, investigators of the RCMP Integrated Tech Crime Unit (ITCU) in C Division (province of Quebec) arrested, following a seven week investigation, a 27-year-old female believed to be at the origin of a botnet, i.e. a group of computers infected by a virus and remotely controlled by a hacker, after conducting a search at her residence located in Saint-Alphonse-de-Rodriguez. Police following a lead found in another case, started gathering open source information on this suspect. With the information found mainly on Youtube, Facebook and on a leaked copy of her hacking forum database, the investigators got enough information to get a search warrant and make an arrest.

The suspect allegedly used malicious software known as Remote Administration Tool (RAT) that allows cybercriminals to remotely take over and control operations of infected computers and to spy on their victims through their web cameras. The investigation shows that the suspect used various methods to harass her victims, including by eavesdropping on private conversations and by communicating with victims through the speakers of their infected computers. She also frightened her victims by taking over control of their computers and by logging on extreme pornography websites. Her victims included underage children both in Canada and abroad. It is also alleged that the suspect posted videos on YouTube in which she can be seen taking over control of infected computers and frightening victims. It is further alleged that the suspect is the owner of an online hacking forum that has 35,000 users worldwide. This Canadian-based forum was also seized. She is facing charges of unauthorized use of computer and mischief in relation to computer data under the Criminal Code.

The Ottawa Police Service (OPS) began an active role in password cracking in February of 2014. Using software and by connecting all computers from local units as well as re-purposing old OPS computers, the array designed is near 100 computers in strength. It is able to bruteforce a SAM (Windows logon) password in excess of 2 billion attempts per second and utilizes idle CPU (Central Processing Unit) and GPU (Graphics Processing Unit) power thus, not impacting officers working on cases.

As encryption is becoming more familiar and widely used by those involved in nefarious activity this array has proven itself invaluable in many investigations. There have been numerous successes with the designed array that without it may have caused files to take a different direction with respect to charges, Some files include a suspect who had numerous password protected archives containing child pornography, the computer suspected of being involved in the swatting incidents across Canada and the USA, and most notably the a file that has recently been in the media which was cracked in 3 days after a change in the algorithm used to defeat a full disk encryption application.
