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
2016 Annual Report

COMMITTEE MANDATE/OBJECTIVE

e crime
committee
CANADIAN ASSOCIATION OF CHIEFS OF POLICE
ASSOCIATION CANADIENNE DES CHEFS DE POLICE

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

2016 Message from the Co-Chairs

The CACP Electronic Crime (e-Crime) Committee Co-Chairs are pleased to report on the 2015/2016 activities. This has been a very hectic year for law enforcement agencies across Canada trying to keep up with the ever-changing fast pace of technology and evolving cybercrime threats. That being said, we are pleased with the accomplishments we have made this year. It would not have been possible to achieve these accomplishments without the subject matter experts within the e-Crime Committee as well as the two sub-committees; the Lawful Access and Electronic Surveillance (LAES) Committee and the National Technological Crime Advisory Committee (NTCAC), now known as the Digital Forensics Committee (DFC). We would like to thank the membership and the two sub-committees with their ongoing dedication and commitment in the support of the e-Crime Committee initiatives.

The e-Crime 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 the Toronto, Montreal, Vancouver, Ottawa, Calgary, Edmonton Police Services and a representative from the Technological Crime Learning Institute from the Canadian Police College. The private and not for profit sectors are represented by the Canadian Bankers Association, Microsoft Canada and the Society for the Policing of Cyberspace. It is important that the Committee works collectively with law enforcement agencies, and with private and not for profit sectors in Canada to provide a national leadership role to the Canadian law enforcement community.

This year the 2016 CACP Annual Conference will take place in Ottawa, Ontario from August 14 to 17, 2016. As cybercrime is at the forefront of law enforcement's agenda, this year's Annual Conference will focus on cybercrime. The theme, **"Public Safety in a Digital Age: Real Victims – Real Crime"**, will help steer discussions towards the growing significance of technology as an evolving threat to public safety in our communities. The e-Crime Committee has worked tirelessly in getting speakers and panelist together for the Annual Conference. The Committee recommended the following sessions for the Annual Conference:

1) The International Law Enforcement Cybercrime Experience – Challenges and Lessons Learned;
2) Partnerships: Industry/Academia/NGOs – Defining the Scope of the Problem (Panel);
3) Meeting the Needs of the Victims of Crime: A Cyber Perspective (Panel);
4) Privacy NOT Anonymity – Find the "Right" Space and not the "Dark" Space (Panel) and;
5) Next Steps: We Can All Do More.

In 2010, the Federal Government released Canada's Cyber Security Strategy, and part of that strategy required the RCMP to develop and produce a Cybercrime Strategy. In December 2015 the RCMP released its Cybercrime Strategy, which sets out an operational framework and an action plan to help Canada's national police service reduce the threat and impact of cybercrime in Canada. Within that framework a National Cybercrime Team was created at the RCMP's National Division in Ottawa. Law enforcement agencies in some of the major cities across Canada are creating cybercrime teams due to the rise in cybercrime complaints. The Committee has drafted a National Cybercrime Strategy in consultation with other Canadian law enforcement agencies, as well as the private sector and other partners. The draft Strategy will be presented to the CACP Board for consideration at the 2016 Annual Conference in August.

A proposal will be made at the 2016 Annual Conference, addressing that cybercrime may be better served by a new Cybercrime sub-committee under the CACP e-Crime Committee. It will be proposed that this Committee will focus upon the operational aspects in the fight against cybercrime. The Committee, if endorsed by the CACP Board, will have representation from law enforcement, private sector, industry, academia and other government departments.

In July 2015, Canada ratified the Council of Europe Convention on Cybercrime also known as the Budapest Convention. The Budapest Convention is an international treaty that provides signatory states with legal tools to help in the investigation and prosecution of computer crime, including Internet-based crime and crime involving electronic evidence. The signing of the Convention has led to an increase in cybercrime requests/assistance from our foreign partners.

In 2016 Deputy Commissioner Scott Tod retired from the Ontario Provincial Police (OPP) and accepted the position of Deputy Chief of Police of the North Bay Police Service. The Committee thanks Deputy Chief Tod for keeping his role and commitment as Co-Chair of the e-Crime Committee after retiring from the OPP. At the 2016 spring meeting, Sgt. Phil Palamattam of the Edmonton Police Service, announced that he would be relinquishing his role as Co-Chair of the DFC in the Fall of 2016. The Committee would like to acknowledge the outstanding contributions of Sgt. Phil Palamattam. A new Co-Chair of the DFC will be selected in the near future.

As Co-Chairs, we would like to thank all the Committee members for their outstanding efforts in the last year and look forward to another challenging year as many law enforcement agencies in Canada will be at the forefront in the fight against electronic crime. With the signing of the Budapest Convention and taking in consideration one of the top priorities indicated by Prime Minister Trudeau's letter to the Minister of Public Safety and Emergency Preparedness in regards to leading a review of existing measures to protect Canadians and our critical infrastructures from cyber-threats, we must ensure that Canadian law enforcement agencies are well equipped to combat online criminals. The Cyber review is critical as the nature of cybercrime is such that no single police service can address alone. Cybercrime is not only a police problem. Cybercrime is a shared responsibility with the private sector, industry, academia and other government departments. We must all work together to combat cybercrime.

Deputy Chief Scott TOD
North Bay Police Service

Chief Superintendent Jeff ADAM
Royal Canadian Mounted Police

PROGRESS ON 2015/ 2016 INITIATIVES:

- **Advance the Cybercrime theme and lead the preparation for the CACP Annual Conference in Ottawa for 2016:** The 111th CACP Annual Conference is being held in Ottawa, Ontario from August 14 to 17, 2016. This year's theme, "Public Safety in a Digital Age: Real Victims – Real Crime" will help steer discussions towards the growing significance of technology as an evolving threat to public safety in our communities. The overall objective is Education and Awareness. Five plenary sessions have been allotted for the e-Crime Committee and the following themes are the topics: The International Law Enforcement Cybercrime Experience – Challenges and Lessons Learned, Partnerships: Industry/Academia/NGOs – Defining the Scope of the Problem (Panel), Meeting the Needs of the Victims of Crime: A Cyber Perspective (Panel), Privacy NOT Anonymity – Find the "Right" Space and not the "Dark" Space (Panel) and Next Steps: "We can all do More".

- **Continue to support the development of a National Digital Field Triage Program:** The e-Crime Committee continues to support the development of a National Digital Field Triage Program (DFT). The Digital Mobile Field Triage (DMFT) and Digital Computer Field Triage (DCFT) programs developed by the RCMP's Integrated Tech Crime Unit in Vancouver has gained in popularity. The DFT program in Vancouver has trained more front line officers in triaging mobile and computer devices and gaining significant momentum as front line officers are able to conduct timely analysis of seized devices at the scene. RCMP Integrated Tech Crime Units in Ottawa and London have conducted several DFT trainings for RCMP units in Ontario based on the successful DFT program currently in place in BC. Ottawa Police Service as well as other law enforcement agencies are also interested in the DFT program. For example the Ontario Provincial Police is rolling out the DFT program in four locations within the Province of Ontario. The Canadian Police College (CPC) will be looking at hosting a train the trainer course depending on the commitment from the law enforcement community. The Committee is recommending the need for developing consistent Standard Operating Procedures and Policy.

- **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 continues to work with Police Information and Statistics (POLIS) Committee and Statistics Canada to advance this initiative in order to ensure that appropriate metrics are collected in regards to cybercrime. The Canadian Centre for Justice Statistics (CCJS) received recommendations from several law enforcement agencies through a questionnaire on cybercrime reporting. POLIS has identified changes required in Niche RMS (Records

Management System) to better capture cybercrime data such as adding mandatory Uniform Crime Reporting (UCR) flags to the incident screen so that any incident in the UCR can be flagged as cybercrime. The Digital Forensics Committee (DFC) formerly known as the National Technological Crime Advisory Committee (NTCAC) is the lead on this initiative.

- **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:** With Cloud services expanding and the increase in an individual's reasonable expectation of privacy relating to searching digital devices creates challenges for law enforcement on criminal investigations. The Committee will be re-visiting this area of concern with the same impact factors as outlined in last year's submissions – impact on investigations. With the re-focus of the new Digital Forensics Committee (DFC) back to pure forensic data, hardware and process concerns, Cloud Computing will be high on the agenda. DFC will be canvassing partners to provide insight on their perspective and solutions to this area and will strive to develop a list of priorities for representative organizations to consider. Commonalities will be established and recommendations will be brought forward as a committee for discussion and presentation to e-Crime. DFC will further envision identifying a potential private sector partner that would not only provide a perspective of Cloud Computing issues in the private sector but give perspective on possible solutions already being considered and implemented.

- **Promote the development of a CACP-lead cybercrime fighting strategy:** The Committee continues to support the development of a National Cybercrime Strategy. In December 2015 the RCMP released its Cybercrime Strategy, which sets out an operational framework and an action plan to help Canada's national police service reduce the threat and impact of cybercrime in Canada. A draft of the CACP-lead Cybercrime Strategy was developed in consultation with other Canadian law enforcement agencies and circulated to the members of the e-Crime Committee for comments. The draft Strategy will be presented to the CACP Board for consideration at the 2016 AGM in August. The Strategy will reflect all Canadian law enforcement agencies fight against cybercrime and to instill confidence in the Canadian public. A proposal will be made at the 2016 AGM that addressing Cybercrime may be better served by a new Cybercrime sub-committee under the CACP e-Crime Committee. It is proposed that this Committee would focus upon the operational aspects in the fight against Cybercrime.

- **Lead a broad project while engaging CACP to ensure e-Crime investigations carried out by Canadian law enforcement agencies are de-conflicted domestically and internationally. A coordinated approach to investigations with international scope (botnet takedown type of investigations) will be developed. Information about training, meetings, and conference opportunities will be shared, ensuring appropriate attendance and value comes from attending:** The Committee is working closely with its stakeholders as in 2015, CACP and National Police Service National Advisory Committee called for the creation of a National Cybercrime Coordination Centre (NC3) for a coordinated Canadian law enforcement response to address cybercrime, provide technical advice and guidance, understand cybercrime in Canada and possibly a compendium of events/conferences that can be shared within the law enforcement community. Perpetrator(s), victims, IT systems and the infrastructure used in a cyber-attack can all be in different jurisdictions which means that Canadian law enforcement agencies need to take a coordinated, national approach to addressing cybercrime. As one of the roles for the NC3, taking a coordinated approach will assist in de-confliction with domestic and international partners. As this is a proposal of a creation of an NC3, this initiative will continue in 2016-2017.

- **Continue to partner with telecommunications companies in order to facilitate future dealings to overcome issues resulting from the Spencer decision and increased fees:** The e-Crime Committee continues to work with the Lawful Access Technical Assistance Compensation Consultative Committee (LATACCC) in relation to trying to establish a common ground for increased fees. Costs levied by telecoms for court ordered services continue to be a topic of discussion and concern. LATACCC is working on a draft proposal establishing a baseline/grid on costs. Currently there are several Telecommunication companies involved in the draft of the baseline costs. This initiative will continue in 2016-2017.

INITIATIVES PLANNED FOR 2016/ 2017:

- **The Cloud Computing – Explore the impact on investigations from forensics to the lawful access of the data storage**

- **Assess impact of encryption on acquired intelligible digital evidence – Going Dark Forum – Define, Scope, Issues and Recommendations**

- **Exploring the deployment of hardware and software as far forward to first responders**

- **Review of SolGen Standards and recommendation for modifications**

- **Continue dialogue with Telecommunication companies through LATACCC in regards to service delivery, fee structure and network intercept capabilities**

- **Proposal for creation of a new Cybercrime Sub-Committee within the e-Crime Committee**

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 DFC 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 2015
CACP e-Crime Committee Meeting
November 4th – 5th, 2015
Quebec City, Quebec

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

- Roundtable introduction of members attending and opening remarks by the Co-Chairs.
- Discussion on CACP 2016 Annual Conference held in Ottawa. The focus at the 2016 Annual will be on Cybercrime.
- Discussion on digital evidence gathering. Supt John Robin presented on “Consolidation of Collection Systems for the RCMP”.
- Presentation by Martin Girard (Bell Canada) of LATACCC on fee structures.
- Presentation by the Chair of the LAES sub-committee. Review of the initiatives and discussion on way ahead for 2015.
- Presentation by the Chair of the NTCAC sub-committee. Review of the initiatives and discussion on way ahead for 2015.
- Presentation on POLCYB (The Society for the Policing of Cyberspace) by Ms. Bessie PANG.
- Discussion on the National Cybercrime Strategy
- Update provided by the co-chairs and discussion on initiatives for 2015-2016. Identification of action items.

Spring 2016
CACP e-Crime Committee Meeting
May 4th – 5th, 2016
Toronto, Ontario

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

- Introduction of all attendees, presentation of the agenda and opening remarks by the Co-Chairs.
- Discussion on CACP 2016 Annual Conference held in Ottawa. Updates on the plenary sessions by the e-Crime coordinators.
- Presentation by Ret. D/Commr. Gary Bass on Cybercrime Statistics Collection.
- Presentation by Warren Silver and Commander Mary Silverthorn of POLIS on Cybercrime Reporting
- Presentation by Martin Girard (Bell Canada) and Dana Adams (Telus) of LATACCC on fee structures.
- Presentation by the Chair of the NTCAC sub-committee. Review of the initiatives and discussion on way ahead for 2016.
  - Discussion on Cybercrime Sub-Committee.
- Presentation by the Chair of the LAES sub-committee. Review of the initiatives and discussion on way ahead for 2016.
- Presentation by Lisa Henderson of MAG CLOC on Computer and Internet-Related Crime Team (CIRCT)
- Update on the the National Cybercrime Strategy by C/Supt. Adam.
- Update provided on the Society for the Policing of Cyberspace (POLCYB) by Ms. Bessie PANG.
- Re-cap and discussion by Co-Chairs on new initiatives for 2016-2017. Identification of action items.

The e-Crime Committee also held three teleconferences since January 2016. The teleconferences served to provide updates on the plenary sessions for the 2016 CACP Annual Conference, finalize agenda items, discuss initiatives and solicit information for the completion of the yearly report. The Committee will also hold a half day meeting on August 14th, 2016 prior to the commencement of the 2016 CACP Annual Conference.

Activities Planned/Significant Dates 2016/2017:

August 14th - 17th, 2016	Submission of 2016 Annual Report Annual CACP Conference Ottawa, Ontario
October 2016	Fall Committee Meeting (TBD) Tentative location – Province of Alberta
Winter 2016	Committee Teleconference (approx. January)
Spring 2017	Spring Committee Meeting (Location TBD)
Summer 2017	Annual CACP Conference
Fall 2017	Committee Meeting (Location TBD)

2016 CACP Annual Conference

The e-Crime Committee was responsible for 5 plenary sessions for this year's 2016 CACP Annual Conference. Below are the sessions in detail being led by the e-Crime Committee members.

MONDAY, AUGUST 15, 2016	
08:00 – 08:45	**The International Law Enforcement Cybercrime Experience - Challenges and Lessons Learned** **Objective** Canada's police services are the primary organizations responsible for investigating cybercrime and for pursuing cyber criminals. Cybercrime is on the rise, both in Canada and internationally. There are few crimes, nowadays, that don't have a digital footprint. One perpetrator can victimize a large number of victims in multiple jurisdictions, often from abroad. Cybercrime requires new ways of policing. Addressing cybercrime requires broad-based domestic and international police cooperation. Canada could benefit from the challenges and lessons learned from the international law enforcement experience in investigating and prosecuting cybercrime cases. What were the challenges and lessons learned in ensuring there was appropriate evidence and addressing challenges in court proceedings in a cybercrime case? **Presenter** Deputy Chief Constable Peter Goodman, National Policing Lead for Cybercrime, Association of Chief Police Officers (ACPO) **Moderator** Chief Superintendent Jeff Adam, Royal Canadian Mounted Police
08:45 – 09:45	**Partnerships: Industry/Academia/NGOs - Defining the Scope of the Problem** **Objective** Panelists will identify examples of where they have good partnerships with Law Enforcement, potential opportunities for stronger ones and provide thoughts on how to best strengthen them. **Presenters** Mr. Dana Adams, Co-Chair, Lawful Access Technical Assistance Compensation Consultative Committee (LATACCC); Director Corporate Security, TELUS International Mr. Patrick Neal, Program Coordinator, Crime & Intelligence Analysis Option

	Forensic Science & Technology, British Columbia Institute of Technology (BCIT) Mr. Kevin Scott, Founder and President, Canadian Identity Theft Prevention Association **Moderators** Ms. Bessie Pang, Executive Director, The Society For The Policing Of Cyberspace (POLCYB) Mr. John Weigelt, National Technology Officer, Microsoft Canada
10:45 – 11:50	**Meeting The Needs of Victims of Crime: A Cyber Perspective** **Objective** The Internet has evolved from something of a novelty to a tool all of us rely upon every day. It has completely changed the way we do things, from how we work to how we communicate, socialise, shop and learn. When we think about how much we depend on the Internet in our daily lives, it's hard to imagine life without it. But everything comes at a price, so the saying goes. The number of people who fall victim to Cybercrime is enormous and sadly, it is getting higher and higher every day. The European Cyber Crime Center (EC3) estimates around 1 million people a day become victims worldwide! Cybercrime has real world long-lasting consequences. This session aims to connect delegates with the realities faced by cybercrime victims including how their lives are affected and the challenges they face in reporting and recovering from virtual crimes in the real world. **Presenters** Dr. Alec Couros, Faculty of Education, University of Regina Ms. Raine Liliefeldt, Director, Member Services & Development, YWCA Canada **Moderator** Ms. Sue O’Sullivan, O.O.M., Federal Ombudsman for Victims of Crime

TUESDAY, AUGUST 16, 2016	
08:00 – 09:00	**Privacy NOT Anonymity - Finding the "Right" Space and not the "Dark" Space** **Objective** Today people and society are challenged with the rapidly changing landscape of technology, privacy and human rights. The expansion of the internet throughout most of the world with mobile devices, and the ability to share massive amounts information in real-time, have challenged both the human and technical law resources of law enforcement. Understanding

	the technology of the internet and the Internet of Things has caused many police and services to adjust their organizational structures, training programs and digital investigative support services. Law enforcement agencies are adapting with limited success to the ever changing landscape of privacy and access to information through the use of technology. Although agencies have been able to adjust and change to technology the decisions associated to digital privacy and technology protection have never been more difficult to understand and appreciate. The way forward for law enforcement leaders is crucial to our success in solving serious and significant crime problems today. **Presenters** The Honourable Justice Jacqueline Loignon, Ottawa, Ontario Mr. Peter Napier, B.A. (Hons.) LL.B., Crown Counsel to Regional Director of Crown Operations, East Region Mr. Douglas Baum, Defence Bar, B.A., LL.B., Addelman Baum Gilbert LLP **Moderator** Acting Superintendent Joan McKenna, Ottawa Police Service

WEDNESDAY, AUGUST 17, 2016	
11:15 – 12:00	**Next Steps: "We can all do more"** **Objective** As we are all aware, cybercrime is borderless which creates challenges for law enforcement to investigate cybercrime. Cybercrime is not only a police problem. Cybercrime is a shared responsibility with the private sector, industry, academia and other government departments. Based on the discussions at the AGM, the recommendations from the Global Studies Group, the Cybercrime review and the Canadian Law Enforcement Cybercrime Strategy we as a Law Enforcement Community are in a better position to combat cybercrime. We can all do more by working together to disrupt and/or prosecute cyber criminals. This session will explore realistic activities that can be undertaken to combat cybercrime by Canadian Law Enforcement agencies. **Presenters** Chief Superintendent Jeff Adam, Royal Canadian Mounted Police Deputy Chief Scott Tod, O.O.M., North Bay Police Service

CACP e-Crime COMMITTEE MEMBERS LIST:

CACP Members	
D/Chief Scott TOD (Co-Chair)	**North Bay Police Services**
C/Supt Jeff ADAM (Co-Chair)	**RCMP Technical Investigation Services**
Paul BEESLEY	Ontario Provincial Police
André BOILEAU	Sûreté du Québec
Darlene SAVOIE	Edmonton Police Service
Myron DEMKIW	Toronto Police Service
Joan McKENNA	Ottawa Police Service
Maury MEDJUCK	RCMP Technical Investigation Services
Ralph PAUW	Vancouver Police Department
Mathieu DURAND	Service de Police de la Ville de Montréal
Sat PARHAR	Calgary 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	
Vern CROWLEY (Secretary DFC)	Ontario Provincial Police
Phil PALAMATTAM (Co-Chair DFC)	Edmonton Police Service
Paulo (Paul) BATISTA (Co-Chair DFC)	Ottawa Police Service
Robert Longstreet (Co-Chair LAES)	Ontario Provincial Police
Hollie RIORDAN (Co-Chair LAES)	Vancouver Police Department
Gurinder DHANOA (Secretary e-Crime)	RCMP Technical Investigative Services
Gareth SANSOM	Justice Canada
France THIBODEAU	Canadian Police College

E-CRIME STORIES 2015-2016

In the last year, Canada has had several high profile cyber related incidents, such as increase in ransomware attacks and the Ashley Madison hack. This rise is due to technology creating new opportunities for criminals. According to Symantec's "Internet Security Threat" report, ransomware attacks in Canada are on the rise. It was reported that Canada ranked fourth on the list of countries hit by ransomware. Ransomware is malware unknowingly installed on a victim's computer that encrypts the user's files. In order to decrypt the files money is asked from the victims, usually in bitcoins.

In December 2015 the RCMP released its Cybercrime Strategy, which sets out an operational framework and an action plan to help Canada's national police service reduce the threat and impact of cybercrime in Canada. Within the framework of the RCMP Cybercrime Strategy was the creation of the RCMP National Cybercrime Team located at National Division in Ottawa, Ontario. By 2018, the Cybercrime team will consist of 21 employees composed of law enforcement and civilian members. The team's focus will be on combatting high priority cybercrime incidents.

In October 2015, Canadian Advanced Technology Alliance (CATAAlliance) partnered with CACP hosted the National Policing Cybercrime Summit in Toronto, Ontario.   The Summit's objective was to add tangible value to the fight against cybercrime by bringing police, industry, government and academic leaders together to exchange information on current cybercrime trends, offer demonstrations of forensic tools, share case studies, and receive updates from experts working in the field, towards the ends of identifying opportunities for a collaborative Canadian response. The e-Crime Committee has fostered a great working relationship with CATA in the fight against electronic crime. RCMP C/Supt. Adam, Co-Chair e-Crime Committee, received the first-ever Weology Leadership Award from CATA in May 2016 for his outstanding work in forming the new e-Crime Committee and leading the national discussion and direction for law enforcement as a collective response to the challenges of cybercrime.

In April 2014, Canada Revenue Agency (CRA) was compromised due the Heartbleed vulnerability. The individual(s) ex-filtrated approximately 900 social insurance numbers from CRA servers. The RCMP National Division Integrated Technological Crime Unit (ITCU) in Ottawa conducted the investigation into the cybercrime incident. The investigation led to the identification of a 19 year old male in London, Ontario. A search warrant was conducted at the residence and numerous items were seized such as mobile devices, tablets, iPods, computers, routers and USB storage devices. The RCMP ITCUs at National Division in Ottawa and at O Division in London, Ontario as well as the Technical Analysis Team at the at the Technical Investigation Services of the RCMP in Ottawa, worked tirelessly to conduct the analysis on the seized devices. The 19 year old male was eventually charged with several Criminal Code offences such as Unauthorized Use of Computer and Mischief to Data relating to the exfiltration of data from CRA and for other breaches. Due to the solid investigation by National Division, in May 2016 the male plead guilty to several of the charges, while other charges were dropped by the Crown. The male was sentenced to an 18 month conditional sentence.

The OPP has implemented a Cyber Strategy based on the three strategic pillars of Prevention, Response and Support. The Strategy's goals include building organizational capacity while ensuring appropriate polices, training and procedures and supports are implemented across the organization to accommodate modern investigations. The center piece of the Strategy is a cyber investigations tiered response model that flows from the initial call for service and progressively involves specially-trained members and units as the complexity of the case increases. Operationalizing the Cyber Strategy involves rolling out a Digital Field Triage Program based on the successful model developed by the RCMP in British Columbia. Additionally, digital forensic analysis is being decentralized to allow for timelier turnaround of evidentiary information.

Through regular contact and liaison with municipal, national and international and private sector colleagues the OPP wants to ensure that its Cyber Strategy and investigations support align with and complement the Canadian Law Enforcement Cybercrime Strategy.

As a response to the rapidly growing area of the internet and technologically based crimes the Calgary Police Service (CPS) stood up its Cybercrime Program with the creation of the Cybercrime Support Team in January 2013. The Calgary Police Service has continued to evolve and expand its Cyber Program over the past three years by increasing the services knowledge and ability to respond to a wide range of cyber and digitally perpetrated crimes. The service now has two Cyber teams (Cybercrime Support Team and the Cyber Investigative Team) along with a Digital Forensics Team (Tech Crime), and a Forensic Video Unit all of which fall under the newly formed Cyber/Forensic Unit in the Technical Operations Section of the CPS.

In October 2015, the Calgary Police Service in conjunction with Alberta Specialized Law Enforcement Training (ASLET) hosted the first Calgary Cybercrime Investigators Summit. This event was a direct response to educate law enforcement as a result of the dramatic rise of online crime in Canada. The Summit provided a venue for information and investigative technique sharing; relationship and partnership development; subject matter expert discussions; best practices development; and review of recent legal implications for online investigations. The two days of instruction offered a local and international perspective on cybercrime investigations based on the expertise of the high-caliber presenters. Calgary Police are working toward hosting a follow up Cybercrime Investigators Summit in the Spring of 2017.

In May 2016, the University of Calgary was the victim of an unidentified ransomware attack. Over 300 workstations, an estimated 60 servers, and thousands of Exchange mail boxes were affected. Subsequent to the infection, 28 BTC or the equivalent $20,000 CDN was paid for decryption keys and data successfully restored. The investigation has revealed that numerous companies and critical infrastructure in North America has been affected by this strain of ransomware/malware. This incident continues to be investigated by the Calgary Police Service, who has partnered with external agencies in both Canada and the United States to assist in the investigation, identification, mitigation and prevention of this malware.

In June 2014, The Toronto Police Service Computer Cyber Crime (C3) was formed as a sub-section of Intelligence Services. At inception, the team consisted of seven uniform members. In 2015, the Computer Cyber Crime increased personnel strength by six members, allowing for coverage twenty hours a day, seven days a week.

In May of 2016, the Toronto Police Service received a report that there was an active Denial of Service (DoS) attack being conducted against the customer Wi-Fi at a popular business location. Technicians for providers of the wireless service were unable to determine the source of the attack. Upon investigation, it was determined that the attack was disrupting wireless access for a large number of restaurants and businesses in the area. Members of the TPS Technological Crime Unit were able to precisely locate the source of the attack. A search warrant was conducted and a variety of networking and computer equipment that was being used to perpetrate the attack was seized. The investigation is ongoing.

Between February 2015 and August 2015, members belonging to an online hacker group known as the Lizard Squad executed approximately thirty-five cyberattacks against American companies during the course of the investigation. These attacks consisted of Denial of Service attacks, resulting in the temporary loss of paid online services, affecting tens of thousands of clients. The affected companies estimate loss in revenue measured in millions of dollars. The Computer Cyber Crime section participated in the on-going investigation, called Project Lulz, which culminated with the arrest of one of the Toronto-based targets in August 2015.

In July 2015, an unidentified group calling itself "The Impact Team" stole the user data of Ashley Madison, a commercial website billed as enabling extramarital affairs. The group copied personal information about the site's user base and threatened to release users' names and personally identifying information if Ashley Madison was not immediately shut down. In August

2015, the group leaked a large amount of company data, including user account details. None of the accounts on the website needed email verification for the profile to be created, meaning that people often created profiles with fake email addresses, and sometimes people set-up accounts for the wrong email address. Toronto Police Service took the lead on the investigation, called Project Unicorn, with assistance from “O” Division ITCU. The case file remains open at this time.

In March 2016, the Ottawa Hospital confirmed that four computers in its network of 9,800 were hit with ransomware which encrypted the information on those machines making it inaccessible to hospital staff. No patient information was affected according to hospital staff and the hospital responded by wiping the drives, and restoring the computers from back-ups. The incident was reported to Ottawa Police Service.