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
2017 Annual Report

COMMITTEE MANDATE/OBJECTIVE

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

2017 MESSAGE FROM THE CO-CHAIRS

The CACP Electronic Crime (e-Crime) Committee Co-Chairs are pleased to report on their 2016/2017 activities. This has been a very challenging 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 three sub-committees: Lawful Access and Electronic Surveillance (LAES) Committee, Digital Forensics Committee (DFC) and the new eCrime Cyber Council (ECC). We would like to thank the membership and the three sub-committees with their ongoing dedication and commitment in the support of the e-Crime Committee initiatives.

In August 2016, the CACP Board of Directors approved a third sub-committee under the E-Crime Committee. The eCrime Cyber Council (ECC) was formed and is composed of members from Industry, non-profit organizations, Academia, Law Enforcement, NGOs and from the Canadian Advanced Technology Alliance (CATAAlliance). The purpose of the ECC is to leverage diverse and well-informed perspectives to recognize and examine current and emerging trends and developments, to connect these perspectives to current and potential research and parallel initiatives, with a view to recognizing opportunities and enabling promising practices in social policy, industry priorities, and technologies that will provide greater safety and security in the cyber world.

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 additionally 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 non-profit sectors in Canada to provide a national leadership role to the Canadian law enforcement community.

At the 2016 CACP AGM, the Co-Chairs presented the National Cybercrime Strategy, which sets out an operational framework and action plan to help Canada's national police service reduce the threat and impact of cybercrime in Canada. The Strategy was drafted in consultation with other Canadian law enforcement agencies, as well as the private sector and other partners. The National Cybercrime Strategy will focus on five pillars: Mainstream, Deter, Collaborate, Enhance and Advocate. The ECC will be responsible to roll out this Strategy.

In recent years, the CACP has studied and published resolutions about a number of key digital policing and cybercrime gaps and challenges. In October 2016, a Government of Canada's Public Consultation on Cyber Security was submitted on behalf of the CACP, which presented

the views of Canadians, the private sector, academics, and other informed stakeholders on the cyber security landscape in Canada. This public consultation supports the Government of Canada's commitment to review measures to protect critical infrastructure and Canadians from cyber threats. It confirmed that cyber security in Canada is a highly complex issue with multiple challenges and an increasing range of opportunities for law enforcement. The responsibility for addressing these challenges and seizing these opportunities is shared by governments, the private sector, law enforcement and the public. The public consultation presented important ideas relevant to cyber security in Canada: the need to uphold Canadians' privacy rights, the need for stakeholders to collaborate with one another (i.e. governments, private sector, law enforcement, academia, non-profit organizations), and the need to rely on cyber security experts. In addition, the Government of Canada's Public Consultation on Cyber Security also yielded recommendations on specific areas for action, needs and means, barriers and constraints. The information gleaned during the consultations will be used to inform the renewal of Canada's Cyber Security Strategy.

As the use of devices and online applications continues to grow, we can expect that online crime will become increasingly sophisticated and varied. That said, law enforcement is becoming aware that emerging technologies create barriers and that they do not have the tools they need. Despite having judicial authority to do so, law enforcement increasingly cannot access the digital evidence needed to support certain types of criminal investigations (e.g. pure cybercrimes). As part of the 2017-2018 sub-committee's planned initiatives that are reported to the e-Crime Committee, there will be a review of the responses to the National Security Consultation in respect to the Investigative Capabilities in a Digital World. Participants that were consulted underlined the importance of addressing the issues arising from difficulties in accessing basic subscriber information (BSI - law enforcement needs timely access to BSI) and from the lack of intercept capabilities (there has been a sharp decrease in the technical capabilities of police to intercept private communications). This also includes issues ranging from the challenges that arise when law enforcement investigations encounter encryption (encryption can pose barriers, such as loss of evidence when law enforcement cannot compel files to be made accessible) to the lack of data retention (which can result in evidence being purged before police can obtain legal authorization to obtain it).

This year, the 2017 CACP Annual Conference will take place in Montreal, Québec from July 15 to July 19, 2017. Building public trust and confidence have become a major focus for policing and new techniques are necessary to accomplish this. The conference theme, "Policing in a Digital Society – Risks and Opportunities" will emphasize insights and tangible deliverables that we will be able to implement in our organizations. The ECC will be holding a panel at this year's AGM on "Cybercrime – Challenges and Lessons Learned".

Deputy Chief Scott Tod announced the relinquishment of his role as Co-Chair of the e-Crime Committee at the 2016 AGM and moving on as Co-Chair of the ECC. The Committee would like to acknowledge the outstanding contributions of D/Chief Tod and wish him continued success as Co-Chair of the ECC. Deputy Chief Sat Parhar of the Calgary Police Service was announced as the new Co-Chair of the e-Crime Committee at the 2016 AGM. D/Chief Parhar

brings with him a wealth of experience and is looking forward to contributing to the great work the Committee is engaged with.

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. One of the main goals in fighting cybercrime, on top of law enforcement responding to cybercrime, will be crime prevention as this is paramount in reducing victimization from cybercrime. The number of people who fall victim to cybercrime is getting higher and higher every day. Ongoing educational awareness campaigns by respected subject matter experts directed at law enforcement, private sector cyber security specialists, businesses and citizens is critical. Taking into account that one of the top priorities indicated in 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, it is essential that Canadian law enforcement agencies are well equipped to combat online criminals. The Cyber review is critical as it supported that the nature of cybercrime is such that no single police service can address it alone. Cybercrime is not only a police problem; Cybercrime is a shared responsibility with the private sector, industry, academia and other government departments. All stakeholders have a responsibility to work together to combat cybercrime as these are real crimes – real victims.

Deputy Chief Sat PARHAR
Calgary Police Service

Chief Superintendent Jeff ADAM
Royal Canadian Mounted Police

PROGRESS ON 2016/ 2017 INITIATIVES:

- **The Cloud Computing – Explore the impact on investigations from forensics to the lawful access of the data storage**
  This area of police investigations is becoming an increasing issue for computer forensics as the availability of cloud storage becomes easier, larger and cheaper to access. This is the equivalent of having the largest capacity storage devices available to anyone at anytime through both static and mobile devices equally well. For computer forensic units this brings two main issues of concern. The first is how to access the data that may or may not be residing on devices and the second is how to deal with the sheer volume of the data. Cloud computing has forced computer forensics to change and adapt the approach to this type of evidence and the tools required to handle this dynamic. The issue comes with added time at scenes to access the data which puts human resource demands on organizations that don't have the resources at all or are already shorthanded and stretched even further. The "legalities" and the jurisdictional hurdles become a side show that also impacts operations and efficiencies. The issue was introduced to the DFC agenda some time ago and it has been forward to the next meeting for discussion due to other agenda items and time constraints.

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

  Like cloud computing, encryption has been evolving over time. Early on the encryption was certainly not as sophisticated as it is presently and there were tools ranging from brute force attacks on passwords to modifying our traditional policing techniques that were moderately successful for policing organizations. With the rapid change of technology, the password cracking capability tools and these special techniques are getting less effective as encryption has evolved and has gotten better, easier to make use of and the data that is increasingly moving towards mobile platforms. Windows operating systems which are by far the largest sector of operating systems offer free encryption tools and Apple products come pre-encrypted now as the default option. Most mobile devices have moved to encryption which has created challenges for law enforcement to decipher the data on these devices.

- **Exploring the deployment of hardware and software as far forward to first responders**
  In answer to ongoing workload problems with computer forensic units and the diverse landscape of the requirement outside the major centers, the issue of Digital Field Triage (DFT) was examined over meetings in late 2015 and leading to a concluding report in the fall of 2016. The problem was to find a recommended process that would allow extraction of data from the devices without burdening the main computer forensic units. If this triage could be pushed to the front line in some way then the analysis and more complicated files could be answered more effectively and efficiently by computer forensic units.
  DFC subcommittee suggested that a program similar to the DFT program currently in

use by the RCMP in British Columbia and supported by the Canadian Police College could form the foundation of this solution. It further defined a structure that would qualify DFT officers with credentials to do:

1. mobile device triage and data extractions on a limited basis or,
2. the ability to preview static devices like laptops and desktop computers,
3. or both.

These DFTs would have to be accredited and accountable to a full computer forensic unit for support, training and follow up as required. It was suggested that this format could be applied to small police organizations or large organizations like the OPP or the RCMP that have widespread commitments run from small resources (detachments). It could also be used by larger centers to alleviate workload and provide a limited 24 hour DFT response similar to the current SOCO program (Scenes of Crime Officers).

- **Review of SolGen Standards and recommendation for modifications**
  The Government is currently preparing to engage in broad public consultations on a range of security and related privacy issues. The consultations will inform the Government's approach to addressing these issues. Given this context, and the need to weigh carefully the full range of implications that updating the SolGen standards could have, we would suggest that any discussions regarding the future of the SolGen standards take place at a later date, after the conclusion of the Government's upcoming consultation process.

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

  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 is an ongoing initiative.

- **Proposal for creation of a new Cybercrime Sub-Committee within the e-Crime Committee**
  As mentioned in the Message from the Co-Chairs, in August 2016, the CACP Board of Directors approved a third sub-committee under the E-Crime Committee. The e-Crime Cyber Council (ECC) will contribute in a wide variety of ways towards the effectiveness of the e-Crime Committee initiatives and share a critical role in ensuring that all are relevant to the needs of the practitioners and innovators that serve them. The ECC supports the CACP e-Crime Committee and the National Cybercrime Strategy's five main pillars: Mainstream, Deter, Collaborate, Enhance and Advocate.

  The duties of the members of the ECC include providing advice and guidance to the CACP e-Crime committee, lead in the execution of core program needs and priorities

as identified in the CACP cybercrime strategy, provide a communication link between ECC efforts and their respective networks/communities, make and act on recommendations which address identified needs, assist in creating partnerships to address identified needs, act as ECC ambassadors, plan/conduct/support advocacy, outreach and awareness raising campaigns, act as ECC Speakers and Thought Leaders at events, webcasts, media interviews etc.

The ECC membership list includes: Accenture, BlackBerry, Bruce Power, Calgary Police Service, Canadian Association of Chiefs of Police, Canadian Centre for Child Protection, Canadian Police College, CATAAlliance, CyberNB, Deloitte Canada, Digital Boundary Group, Durham Regional Police Service, Global Network for Community Safety, HumanLed, Inc. Magnet Forensics, MNP Inc., National Cyber Forensics and Training Alliance Canada, North Bay Police Service, Ontario Provincial Police, Peel Regional Police Service, Royal Canadian Mounted Police, Service de police de la ville de Montréal , Smart Cybersecurity Network (SERENE-RISC), UNISYS, and Vancouver Police Department.

INITIATIVES PLANNED FOR 2017/ 2018:

- A resolution supporting the reform of s. 487.11 to include the following Criminal Code provisions:

  492.2 [Transmission Data Recorder]

  492.1(2) [Tracking an Individual's movement by identifying the location of a thing that is usually carried or worn by the individual]

- Coordinating and Educating Law Enforcement's approach to consistent standard operating practices and the articulation of the use of sensitive tools within judicial authorizations
- A review of the responses to the National Security Consultation in respect to the Investigative Capabilities in a Digital World:
  a. Basic Subscriber Information;
  b. Intercept Capabilities by Communication Providers
  c. Encryption
  d. Data Retention

  With a view to producing a document to address any misconceptions in those responses.
- Continue to look at the developing issues around cloud computing in an effort to further identify the problem and give recommendations for best practices and procedures.
- Review the benefits and impacts of lab accreditation on Canadian police organizations and operations.
- The issue of data retention policy with respect to digital forensics has been an ongoing discussion. DFC will further examine the retention policy in an effort to come up with a "best practices" guidelines.
- Continue to move the DFT program out to the front line officers in Canada.
- CATA/ECC will be organizing an International Cybercrime Summit in 2017 themed on five pillars: Mainstream, Deter, Collaborate, Enhance and Advocate.
- Regional Cyber Workshops for Building Capacity for local police services, industry, local business partners and the public.
- Resolution calling for the creation of a national reporting function for victims of cybercrime
- Assess, assist and advocate on matters related to educating all law enforcement personnel on cybercrime investigation techniques
- Mainstream cybercrime prevention techniques and awareness through dedicated outreach campaign.

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, DFC and ECC 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 2016
CACP e-Crime Committee Meeting
October 27th, 2016
Calgary, Alberta

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

- Roundtable introduction of members attending and opening remarks by the Co-Chairs.
- Update on the 2016 Annual Conference held in Ottawa, Ontario in August.
- Discussion on Going Dark and Cybercrime. Raise public confidence that Canadian Law Enforcement Agencies are working on combatting cybercrime.
- Discussion on the National Cybercrime Strategy.
- Presentation by the Co-Chairs of the ECC sub-committee. Review of the initiatives and discussion on way ahead for 2016-2017.
- Discussion on the National Cybercrime Strategy.
- Presentation by Karen Audcent (DOJ) and Nick Koutrous (ISED) on Lawful Access and National Security Consultation Review.
- Presentation by the Co-Chairs of the LAES sub-committee. Review of the initiatives and discussion on way ahead for 2016-2017.
- Presentation by the Co-Chair of the DFC sub-committee. Review of the initiatives and discussion on way ahead for 2016-2017.
- Presentation by POLIS with respect to an update on cybercrime reporting.
- Update provided by the co-chairs and discussion on initiatives for 2016-2017. Identification of action items.

Spring 2017
CACP e-Crime Committee Meeting
May 3rd, 2017
Montreal, Quebec

The spring meeting of the CACP e-Crime was hosted by the Service de police de la Ville de Montréal. The below points outline the topics discussed during the meeting:

- Introduction of all attendees, presentation of the agenda and opening remarks by the Co-Chairs.
- Presentation by Co-Chairs of the ECC sub-committee. Review of the initiatives and discussion on way ahead for 2017.
- Presentation by the Co-Chairs of the LAES sub-committee. Review of the initiatives and discussion on way ahead for 2017.
- Presentation by the Co-Chairs of the DFC sub-committee. Review of the initiatives and discussion on way ahead for 2017.
- Presentation by Randy Schwartz of the Ontario Ministry of the Attorney General on recent Supreme Court of Canada cases.
- Presentation by LATACCC on fee structures.
- Discussion on Sensitive Techniques – Protection & Transparency.
- Re-cap and discussion by Co-Chairs on new initiatives for 2017-2018. Identification of action items.

Activities Planned/Significant Dates 2017/2018:

July 16th - 19th, 2017	Submission of 2017 Annual Report Annual CACP Conference Montreal, Quebec
October/November 2017	Fall Committee Meeting Vancouver, BC
November 6-8	2nd International Cybercrime Summit Courtyard Marriott East Ottawa, Ontario
Spring 2018	Spring Committee Meeting (Location TBD)
Summer 2018	Annual CACP Conference
Fall 2018	Committee Meeting (Location TBD)

CACP E-CRIME COMMITTEE MEMBERS LIST:

CACP Members	
D/Chief Sat Parhar (Co-Chair)	**Calgary Police Services**
C/Supt Jeff ADAM (Co-Chair)	**RCMP Technical Investigation Services**
Scott TOD (Co-Chair ECC)	North Bay Police Service
Paul BEESLEY	Ontario Provincial Police
Nathalie MARTIN	Sûreté du Québec
Darlene SAVOIE	Edmonton Police Service
Myron DEMKIW	Toronto Police Service
Jim ELVES	Ottawa Police Service
Maury MEDJUCK	RCMP Technical Investigation Services
Joanne WILD	Vancouver Police Department
Mathieu DURAND	Service de Police de la Ville de Montréal
Ryan JEPSON	Calgary Police Service
Uday JASWAL	Durham Regional Police Service
CACP Associate members	
Kevin Wennekes (Co-Chair ECC)	CATAAlliance
Malcolm CHIVERS	Canadian Bankers Association
Bessie PANG	Society for the Policing of Cyberspace (Polcyb)
John WEIGELT	Microsoft Canada
Alan TREDDENICK	Blackberry
Technical Advisors	
Gurinder DHANOA (Secretariat e-Crime)	RCMP Technical Investigative Services
Hollie RIORDAN (Co-Chair LAES)	Vancouver Police Department
Robert Longstreet (Co-Chair LAES)	Ontario Provincial Police
Brandt WATKINS (Co-Chair DFC)	Vancouver Police Department
Paulo (Paul) BATISTA (Co-Chair DFC)	Ottawa Police Service
Frank D'AOUST	Ottawa Police Service
Vern CROWLEY	Ontario Provincial Police
France THIBODEAU	Canadian Police College
Gareth SANSOM	Justice Canada

E-CRIME STORIES 2016-2017

In 2016-2017, ransomware was still one of the top cyber threats to businesses and citizens around the world. According to ComputerWeekly.com, in May 2017, the WannaCry ransomware was a global attack that affected more than 200,000 computers in over 150 countries. During 2016-2017 Canadians were not immune to ransomware and other email threats, malware and botnets. With the evolution of Internet of Things (IoT) and smart cities, many systems will be interconnected and Canadians will have to ensure they are safeguarded from possible new vulnerabilities.

In December 2015, the RCMP released its Cybercrime Strategy which included the creation of a Cybercrime Investigative Team (CIT). The CIT, currently housed within the Technological Crime Unit at the National Division of the RCMP, is currently in its third year of implementation. The CIT has been hard at work building its capacity, and is well positioned to complete all staffing of personnel in the coming months. Members of the team are building strong expertise in the different facets of Cybercrime investigations. CIT members are currently conducting four priority investigations, two of these files are expected to result in charges in the coming months. These charges will be laid against Canadians directly involved in targeting computers systems for monetary profit. In addition to these four priority files, the team is also busy investigating approximately 20 other investigations currently at various stages of completion. The CIT is expected to be fully operational by the end of 2017 and will continue to tackle Cybercrime which unfortunately continues to victimize Canadian citizens on a much too routine manner.

In 2015 the RCMP Cybercrime Strategy identified the need to increase capacity in Cybercrime training at the Canadian Police College. The Technological Crime Learning Institute (TCLI) at the CPC was given four new positions to fulfill that mandate. Currently the TCLI has 10 members to deliver technological crime training and with the addition of the new members, the TCLI has introduced the Cybercrime Investigative Technique Course, the Advanced Open source intelligence Course, revamped the Cell phone Search and Seizure Course to the newly created Mobile Device Acquisition and Analysis Course. In addition, TCLI has doubled the delivery of existing courses to reduce the demand and to offer more options to our clients. More details on these and other courses offered at the TCLI can be found on their website at www.cpc.gc.ca.

One of the initiatives that the E-Crime Committee is reviewing is the rollout of the Digital Field Triage program nationally for municipal and local law enforcement agencies. The RCMP is currently working on rolling out the DFT program within its own jurisdictions in the Provinces and Territories. The CPC has been engaged to look into how this training could be delivered nationally. The initiative is still in the planning stage and discussions are ongoing with RCMP Technical Investigation Services in Ottawa with respect to delivery of the DFT program and training. TCLI is looking to deliver the first DFT train the trainer training in late 2017.

In 2015 Montreal RCMP (C Division) Integrated Tech Crime Unit started a joint investigation on the Avalanche network with international partners (Europol, United Sates and Germany).

Avalanche dates back to 2008-2009 and has distributed at least 20 families of malware typically banking trojans directed at various banking systems. Avalanche was a double fast flux Botnet that moved key portions of its infrastructure every 6 months. In 2012 the State Police in Verden Germany had received some 3400 criminal complaints and local banks had lost millions of Euros to various banking trojans spread by Avalanche. In 2016 Avalanche was spreading GozNym which IBM estimated was costing the USA $2,000,000/day.

By 2015 the Avalanche Botnet file was coordinated by Europol and C division had received a number of MLAT requests. Avalanche had moved from northern Europe to the USA and was presently targeting USA banks. In 2015 and 2016 C Division obtained judicial authorization for production orders and Transmission Data Recorder (TDR) orders for 3 local web service providers. The top level servers were now located in Canada and with the TDR information shared via Europol, authorities were able to map all of the Avalanche network and begin planning it`s take down and the arrest of 20 individuals most of whom were located in Eastern Europe.

The take down was pushed back to November 30th, 2016 given the size of the Botnet and the efforts it would take to sinkhole. In the sinkholing efforts C division obtained judicial authorization to seize (block) 101 Canadian machine generated URLs at CIRA. Several Canadian command and control servers were seized via warrant in Quebec and Ontario.

The Botnet was successfully sinkholed by Shadowserver org. and had over 800,000 infected hosts. The November 30th, 2017 takedown and arrests would not have been possible without the joint investigation and sharing of information by all involved that was coordinated through Europol. The seizing of Domain Generation Algorithms (DGA) domains was a first in Canadian law enforcement and could be a useful tool in further botnet files.

The RCMP's use of cell-site simulator (CSS) technology has been the subject of recent misperception and confusion by the Canadian public and the media. On April 5th, 2017, the RCMP publicly confirmed the use of CSS to conduct MDI activities, in certain investigations and further clarified how they are used in the interest of being transparent and improving the public's understanding of the RCMP's use of this technology. As Canada's national police force, the RCMP uses various technical investigative tools and methods to lawfully obtain evidence in order to protect Canadians and investigate serious crimes, MDI activities are just one of them. As well on April 5th, 2017, the opportunity presented itself to re-iterate that the RCMP's MDI technology is not capable of collecting the contents of any form of private communication. It cannot collect the content of voice and audio communications, email messages, text messages, contact lists, images, encryption keys, or any other content and basic subscriber information. CSS's remains a critical tool for the RCMP to identify a suspect's mobile device, allowing investigators to gather valuable evidence and further an investigation. The RCMP also recognizes the need to protect sensitive tools and techniques while balancing public transparency and disclosure requirements to the courts.

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 policies, training, procedures and resources are implemented across the organization in support modern investigations.

The Cyber Strategy supports 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 investigation increases.

Operationalizing the Cyber Strategy includes many initiatives such as the Digital Field Triage Program, the Employee Internet Access Program, the creation of a Cybercrime Investigations Team to deal with cybercrimes where technology is the target and decentralizing digital forensics to allow for timelier turnaround of evidentiary information.

Through regular collaboration with municipal, national and international law enforcement agencies, academia and the private sector, the OPP will ensure that it's Cyber Strategy and investigations align with and complement the Canadian Law Enforcement Cybercrime Strategy.

The Calgary Police Service continued to implement its cybercrime strategy by building partnerships with the community and industry throughout 2016 and 2017. The Service's Cybercrime Education Officer provided 200 presentations on cybercrime to more than 17,000 students, parents, educators and agencies in Calgary between 2016 and the first half of 2017. Thirty presentations were delivered by members of the Cyber/Forensics Unit at conferences, private sector organizations and individual companies focused on building trust between the police and businesses. This has resulted in a reporting increase to CPS in cases related to cyber-fraud as well as an improved mechanism to share threat intelligence. The Service is developing 'cyber academies' aimed at increasing the level of knowledge of cybercrime and prevention strategies to reduce victimization among Calgarians and specifically within small-medium sized businesses.

The CPS Cyber/Forensics Unit continues to support officers and investigations in the collection and analysis of digital evidence. Internal training courses have been developed to ensure officers are aware of their lawful authority and limitations when investigating crimes involving the internet such as stolen property offered in online sales forums. A cybercrime investigators summit is planned for March 2018 to provide training to general investigators as well as subject matter experts on best practices and emerging trends in investigations involving digital evidence.