Executive Report to the CACP Board of Directors
… from CACP Global 2015

Cyber crime: Police Roles and Responsibilities Within a Collaborative Framework

In the fall of 2014, the CACP Board of Directors assigned to the newly rebranded CACP Executive Global Studies Program (CACP Global) the research task of examining cyber crime in both a domestic and global context. In framing this assignment, the board recognized cyber crime as an emerging concern “*that challenges the traditional skills, capacities, roles and response patterns of policing …* “ and further highlighted that “ *… the need for a coherent national response is an emerging priority for Canadian police leaders*.” Beginning in January, the 2015 cohort of 17 succession-ready police leaders embraced this challenge. The CACP Global 2015 cohort included representatives from 11 federal, provincial, local and military policing agencies, and in keeping with the tradition of the prior seven cohorts, they pursued this research challenge within a transformative learning framework, following a problem-based approach.

After over seven months of domestic research and global field studies, intensive online interaction and residential workshops, the cohort will introduce at the CACP Annual General Meeting and National Conference in Quebec City, six related products which together form the deliverables of the CACP Executive Global Studies Program 2015.

1. CACP Global 2015 Executive Report – this brief document;
2. Cyber crime: Let’s Get on With It – a living document, the Appendix to this executive summary that chronicles the state and evolution of the cohort’s research, and which serves as a more detailed record of the issues and observations that have formed the other deliverables;
3. CACP Global 2015: An Action Guide on Cyber Crime for Canadian Policing – a quick reference guide for executives and members at all levels of policing, providing immediate suggestions on how everyone in policing can do more to address the challenge of cyber crime (English version attached – to be distributed in both official languages during the conference and afterward via the national office);
4. CACP Resolution #07-2015: Cyber Crime: Police Roles and Responsibilities Within a Collaborative Framework – slated for consideration in August 2015 at the upcoming Annual General Meeting (see Page 4 of the Guide attached);
5. Cyber Crime: Shaping a Multi-level Response from Canadian Policing – a 30 minute presentation and panel discussion to be delivered within the Professional Program of the CACP Annual Conference;
6. Cyber Crime: Let’s Get On With it – a CACP Take 5 video production that will introduce the conference presentation, and which will serve as a continuing catalyst for discussion and increased awareness across Canadian policing.

Along with marking the successful conclusion of the formal component of the cohort's work, these deliverables are intended to illuminate a way forward on cyber crime for the Canadian law enforcement community, properly situated within a wider, collaborative whole-of-society response to this type of increasingly prevalent and pernicious crime.

The core message in all of these deliverables is both consistent and relatively simple: cyber crime is a crime that victimizes our citizens; policing at all levels of society must be part of the response; and the time to tackle it is now. This document will briefly describe the work undertaken by the cohort and summarize the attached and related products.

Our Approach to the Study

As a first step, the cohort conducted a ground-clearing exercise to define the problem; review literature; and, establish a domestic baseline assessment of the problem. This exercise, which was conducted and discussed with representatives from the CACP's e-Crime and International Committees, established that the scale of the "cyber" is vast; there is a lot of ongoing "cyber" related work locally, nationally and internationally; and that this activity faces 8 enduring challenges in the Canadian context:

- definition ("what is cyber");
- police capacity;
- police competency;
- coordination and de-confliction;
- police jurisdiction;
- legislative gaps and opportunities;
- public dialogue; and,
- the coming future.

This baseline analysis, and resulting discussions with several visiting panels of experts, helped the cohort to hone in on a research objective and to establish a set of research dimensions as a framework through which to consider the question put to it by the Board of Directors. Specifically, the cohort decided **"to examine approaches in certain other countries to identify the most effective roles for police within a collaborative framework."** In examining these approaches, the cohort aimed to look at a variety of dimensions including:

- the extent and impact of cyber victimization (does anyone have a good bead on the scope of the problem),;
- strategic approaches (what are other countries aiming to do: harden targets, increase awareness, catch bad guys);
- the success factors and sustainability of a collaborative approach to cyber crime (who should be at the table and what makes the table work);
- roles and responsibilities for cyber crime (what role do the various levels of law enforcement play, what about the private sector);
- societal attitudes (how does the public outside of Canada perceive the challenge); and,
- evaluations (how do we know we're making progress).

Our Global Study in Cyber Crime

With these dimensions in mind, the cohort next conducted a global scan for countries that could yield potential lessons for Canada. Nine countries were ultimately selected for site visits, and sub-teams were formed to complete the field studies, as follows:

The United Kingdom and Spain
France, Germany, and the Netherlands
India and Singapore
Australia and New Zealand

These countries were chosen for a range of reasons, ranging from best practices to emulate, to instructive bellwethers of the challenges yet to come to Canada. For example, the UK, Australia and New Zealand were selected because of the similarity in their approaches to policing and the state of their cyber-preparedness. The Netherlands and Singapore were selected because research had suggested that Europol's EC 3 centre and Interpol's Global Complex for Innovation were best practices in collaboration worth examining. India, on the other hand, was selected because of its rapidly expanding technology sector, and because it is a key source country for email spam and other forms of malicious cyber activity.

The cohort conducted its site visits between late March and early May 2015. Teams conducted in-depth, structured field interviews with almost 100 experts representative of policing, government, academia, and private industry during these visits.

In addition to the field studies, the full cohort hosted several delegations during its residential study periods, allowing the team to engage with, among others:

- A senior representative of the Pittsburgh-based National Cyber Forensics and Training Alliance (NCFTA) to ensure that the whole cohort would benefit from a first-hand appreciation of the US experience in cross-sector public-private collaboration;
- Representatives of the still-forming, Toronto-based JORM initiative on Cyber Crime, bringing both policing (financial crimes) and bank executive perspectives on emerging strategies in the banking sector;
- Representatives of the Montreal-based Canadian National Cyber Forensics and Training Alliance (NCFTA), who showcased advanced research and tracking tools being developed and tested for use in Canada.

Synthesizing Key Takeaways from What We Saw

Each country yielded valuable insights and there were several common themes evident across all countries studied. These themes also resonated very strongly against our earlier Canadian baseline analysis, and included:

- the staggering scale of the problem;
- the vital importance of close relationships between police and industry;

- the urgent need to increase reporting of cybercrimes to police;
- the need to improve information sharing among all actors;
- the lack of cybercrime awareness among the general population;
- the lack of necessary skill sets among police;
- the lack of necessary knowledge among the judiciary, and criminal justice practices that are inadequate to investigating and prosecuting cybercrime;
- the lack of common metrics to measure cybercrime and its impacts;
- the growing importance of coordination and de-confliction; and
- the futility of pursuing border-based solutions for what is effectively a borderless category of crime.

We next considered these observations through the lens of a number of theoretical models in an attempt to best synthesize applicable lessons for Canada. At first, the cohort considered cyber crime as *public health problem,* where addressing the spread of a disease (in this case online crime) requires a systems-based approach, drawing on an ecology of interrelated actors, with a focus on systemic prevention. Under such a model, the role for policing might best be described as controlling outbreaks and effectively *quarantining* those spreading the disease.

We next considered a standard "4 Ps" strategic approach – prepare, prevent, pursue and protect. This approach was showcased in the UK and is similar to strategies for other contemporary security challenges such as Canada's counter-terrorism strategy. This approach seemed abstract to the cohort as it seemed more appropriate to, and placed more emphasis on, non-police roles.

In turn, we focused on a model that was observed in Germany at the German Competence Centre against Cyber Crime (G4C). G4C's approach to cyber crime focuses on increasing the complexity of committing attacks, increasing the cost to offend, and reducing the reward for offenders. This approach resonated strongly with the cohort because of its simplicity and its similarity to more traditional policing approaches to crime, generally.

This final approach also led the cohort to its ultimate conclusion: *that tackling cyber crime is about recognizing it as crime*, and as a result, *the traditional crime model is the most appropriate prism through which to address it*. An approach to cyber crime which focuses on a police response that is framed around the three key elements of the basic crime model – *the offender, the victim, and the location and/or opportunity for the crime* – would go a long way to de-mystifying the view that cyber crime is something more complex than what it truly is.

Expressing Our Three Truths About Cyber Crime

Thus, to provide a frame for our ultimate recommendations for action, we believe the following three truths first need to be expressed, amplified and better understood across Canadian policing:

> Cyber crime is crime … and it is creating victims with often devastating impacts.
> Cyber crime is a community safety priority, everywhere.
> Cyber crime is actionable, to some degree, at all levels of policing.

Our Recommendations to Canada's Policing Community

Within this framework – *built upon the recognition that cyber crime is just crime in the twenty-first century* – the members of CACP Global 2015 arrived at six key recommendations that we believe are applicable to and actionable by police leaders at all levels of Canadian law enforcement:

1) **Mainstream "cyber"**

   A paradigm shift is needed. Law enforcement needs to train the public facing aspects of its services to recognize crime online as crime that is impacting their citizens, and to encourage its reporting.

   Investigative capability to address the online world in general investigative units needs to be established and fostered. Dealing with the online world cannot be left to specialist units.

2) **Increase community awareness and victim support**

   In recognizing that it is a crime, law enforcement needs to provide support to victims. It also needs to increase awareness about how to avoid being victimized. Like with other crimes and other community safety concerns, this is probably best done through educating youth early and often. That doesn't mean that law enforcement has to own the problem. Existing initiatives like *getcybersafe.ca* are powerful resources that police can draw upon. CACP should consider a "Cyber Safety Day" equivalent to National Prescription Drug Drop-off Day.

3) **Extend trust and collaboration beyond law enforcement**

   Canada needs to formalize a robust model for collaboration across sectors. Co-location with appropriate information sharing protocols is the ideal and, though it brings with it a certain level of risk, it is achievable within current legislative frameworks.

   We should leverage, restructure and/or realign existing structures and initiatives into a consolidated approach. This should be done quickly to stop further fragmentation of the Canadian response into a messy quilt of coordination centres.

4) **Establish mechanisms and structures to achieve coordination and information sharing at local, provincial, national and international levels**

   Canada lacks mechanisms and structures seen in other countries to achieve coordination and information sharing at local, provincial, national and international levels.

   Online crime challenges current deployment models, authorities and jurisdictions. A Federal-Provincial-Territorial conversation about addressing the borderless nature of online crime is urgently needed to overcome the constitutional dispersal of Canadian policing.

5) Enhance capability and capacity of the judicial system

We need to address capability and capacity of law enforcement and the judicial system in a variety of ways, including:

- training -- digital basics should be included in all cadet training, specialized in-service training is needed, as is training for specialized prosecutors;
- investigative capacity -- regional cyber crime investigative teams are needed;
- tools -- digital forensics tools need to be pushed to the frontline;
- recruiting – non-traditional recruiting strategies should be examined.

6) Advocate for certain legislative and regulatory changes

Continued legislative reform is required to keep pace with changing technology and the online environment. Most urgently, data preservation standards are required to address the latest trends of corporations to hold data for shorter and shorter periods of time. Similarly, powers to enable domestic production orders for foreign data would greatly streamline a range of investigations. At the same time continued advocacy for effective lawful access and increased efficiencies to the MLAT process are critical to being future ready.

It is with these recommendations in mind that the cohort has crafted Resolution #07-2015 for consideration at the upcoming AGM. We believe it captures the spirit of the CACP Global 2015 cohort's recommendations, and that it further leverages the existing and continuing work of the CACP e-Crimes committee. Ultimately, we believe the Resolution amounts to a necessary call on the CACP to embrace one summarizing message that derives from this extensive global study:

Cyber crime in Canada: let's get on with it.

> *"[Cyber Crime]…It's like salt in your food. It is in everything"*
>
> - *Insp. Gupta, Central Bureau of Investigation Academy, India*