CACP Global 2015

An *Action Guide* on Cyber Crime for Canadian Policing

CACP EXECUTIVE GLOBAL STUDIES PROGRAM

PROGRAMME D'ÉTUDES INTERNATIONALES POUR CADRES SUPÉRIEURS ACCP

CANADIAN ASSOCIATION OF CHIEFS OF POLICE · ASSOCIATION CANADIENNE DES CHEFS DE POLICE

THREE TRUTHS ABOUT CYBER CRIME

IT IS A CRIME

- It has real victims who often face devastating impacts
- It often has links to Organized Crime or other criminality
- It is a threat to the rule of law

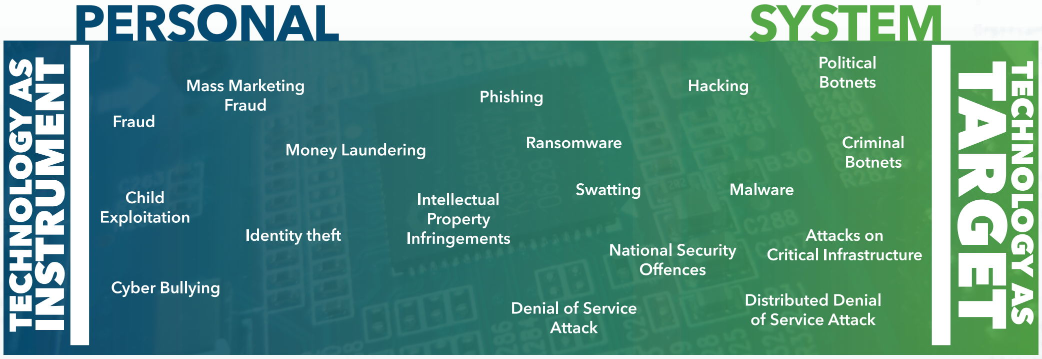
IT IS A COMMUNITY SAFETY PRIORITY BECAUSE:

- It is under reported and too rarely investigated
- It is causing real harm in our communities
- The intensity of victimization is growing rapidly
- It is only going to get worse with technological innovation

IT IS ACTIONABLE AT ALL LEVELS OF POLICING

- When there is a collaborative approach
- When there is coordination
- When police have the knowledge and skills necessary

THE POLICING SPECTRUM IN CYBER CRIME



PERSONAL

SYSTEM

TECHNOLOGY AS INSTRUMENT

TECHNOLOGY AS TARGET

Fraud

Mass Marketing Fraud

Money Laundering

Child Exploitation

Identity theft

Cyber Bullying

Intellectual Property Infringements

Phishing

Ransomware

Swatting

Denial of Service Attack

National Security Offences

Hacking

Malware

Political Botnets

Criminal Botnets

Attacks on Critical Infrastructure

Distributed Denial of Service Attack

Higher Police Understanding
Generalized Response Needed

Lower Police Understanding
Specialized Response Needed

Cybercrime comes in many forms. All forms are crime.

GLOSSARY OF TERMS

BOTNET
A collection of compromised computers (bots) running malicious applications without the knowledge of the user via a command and control infrastructure.

DECONFLICTION
In the context of cyber crime, avoiding redundancy, interference and/or investigative conflicts among the actions and systems of various agencies.

DENIAL OF SERVICE ATTACK (DOS)
A type of cyber-attack aimed at overwhelming or otherwise disrupting the ability of the target system to receive information and interact with any other system.

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)
In a DoS attack, one computer and one internet connection is used to flood a server with packets, with the aim of overloading the targeted server's bandwidth and resources. A DDoS uses many devices and multiple Internet connections, often distributed globally and often hijacked into what is referred to as a botnet.

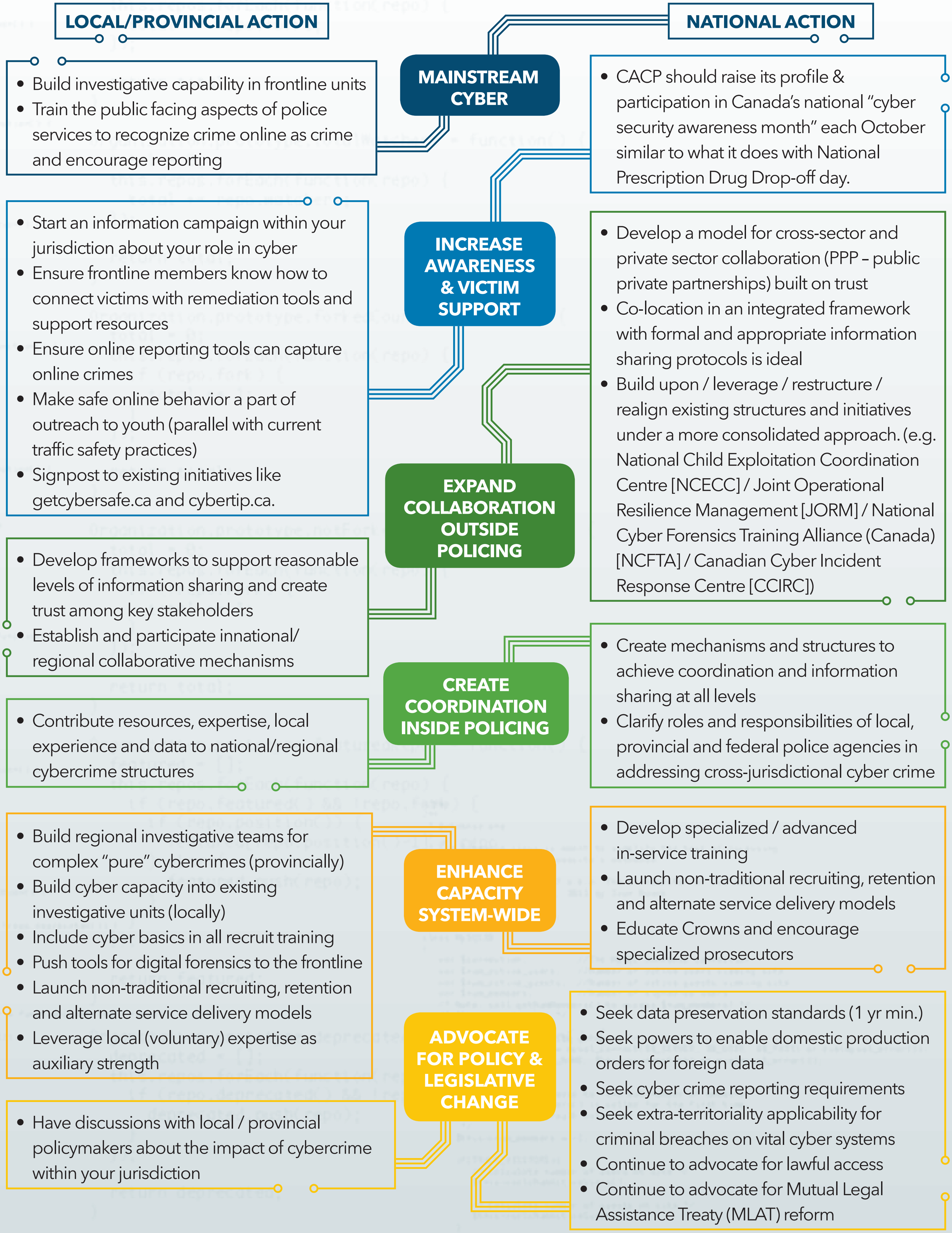
HACKER
Someone who uses computers and the Internet to access computers and servers without permission.

MALWARE
Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware, and adware.

RANSOMWARE
Software that denies you access to your files until you pay a ransom.

SWATTING
Swatting is an internet prank/crime where someone finds your address either through your Internet Protocol or because your name and location is known. Then they call 911 anonymously and report a fake emergency.

WE CAN ALL DO MORE - A SHIFT IS CALLED FOR ACROSS CANADIAN POLICING



LOCAL/PROVINCIAL ACTION

NATIONAL ACTION

MAINSTREAM CYBER

- Build investigative capability in frontline units
- Train the public facing aspects of police services to recognize crime online as crime and encourage reporting

INCREASE AWARENESS & VICTIM SUPPORT

- Start an information campaign within your jurisdiction about your role in cyber
- Ensure frontline members know how to connect victims with remediation tools and support resources
- Ensure online reporting tools can capture online crimes
- Make safe online behavior a part of outreach to youth (parallel with current traffic safety practices)
- Signpost to existing initiatives like getcybersafe.ca and cybertip.ca.

- CACP should raise its profile & participation in Canada's national "cyber security awareness month" each October similar to what it does with National Prescription Drug Drop-off day.

EXPAND COLLABORATION OUTSIDE POLICING

- Develop frameworks to support reasonable levels of information sharing and create trust among key stakeholders
- Establish and participate innational/ regional collaborative mechanisms

- Develop a model for cross-sector and private sector collaboration (PPP – public private partnerships) built on trust
- Co-location in an integrated framework with formal and appropriate information sharing protocols is ideal
- Build upon / leverage / restructure / realign existing structures and initiatives under a more consolidated approach. (e.g. National Child Exploitation Coordination Centre [NCECC] / Joint Operational Resilience Management [JORM] / National Cyber Forensics Training Alliance (Canada) [NCFTA] / Canadian Cyber Incident Response Centre [CCIRC])

CREATE COORDINATION INSIDE POLICING

- Contribute resources, expertise, local experience and data to national/regional cybercrime structures

- Create mechanisms and structures to achieve coordination and information sharing at all levels
- Clarify roles and responsibilities of local, provincial and federal police agencies in addressing cross-jurisdictional cyber crime

ENHANCE CAPACITY SYSTEM-WIDE

- Build regional investigative teams for complex "pure" cybercrimes (provincially)
- Build cyber capacity into existing investigative units (locally)
- Include cyber basics in all recruit training
- Push tools for digital forensics to the frontline
- Launch non-traditional recruiting, retention and alternate service delivery models
- Leverage local (voluntary) expertise as auxiliary strength

- Develop specialized / advanced in-service training
- Launch non-traditional recruiting, retention and alternate service delivery models
- Educate Crowns and encourage specialized prosecutors

ADVOCATE FOR POLICY & LEGISLATIVE CHANGE

- Have discussions with local / provincial policymakers about the impact of cybercrime within your jurisdiction

- Seek data preservation standards (1 yr min.)
- Seek powers to enable domestic production orders for foreign data
- Seek cyber crime reporting requirements
- Seek extra-territoriality applicability for criminal breaches on vital cyber systems
- Continue to advocate for lawful access
- Continue to advocate for Mutual Legal Assistance Treaty (MLAT) reform

Every Canadian police service should be actively promoting these resources in every community: www.getcybersafe.gc.ca

CACP RESOLUTION #07-2015

CYBER CRIME: POLICE ROLES & RESPONSIBILITIES WITHIN A COLLABORATIVE NATIONAL FRAMEWORK

Sponsor: CACP Executive Global Studies Program 2015
Norman E. Taylor, Program Director

WHEREAS as proposed in Resolution #03 – 2012, and through the continuing work of the e-Crimes Committee, the CACP has called on the Government of Canada, together with its public and private sector partners to develop a National Cybercrime Strategy to disrupt cybercrime; and,

WHEREAS in August 2014, the CACP Board of Directors further recognized cybercrime as an emerging concern stating, it is "a topic that challenges the traditional skills, capacities, roles and response patterns of policing … the need for a coherent national response is an emerging priority for police leaders"; and,

WHEREAS current empirical evidence suggests that solutions to cyber-based victimization demand effective collaboration among multiple actors, and that all levels of policing share unique responsibilities to protect citizens and to uphold the rule of law; and,

WHEREAS the CACP Global Executive Studies Program 2015 was directed by the CACP Board to research and illuminate a way forward for Canada on cybercrime by studying approaches in selected key countries to identify the most effective roles for police within such a collaborative framework; and,

WHEREAS in May 2015, after research and field interviews with almost 100 experts in nine countries representative of policing, government, academia, and private industry, the Global Studies cohort concluded that the most promising law enforcement responses to cybercrime are characterized by:

(1) Addressing cyber crime as a core policing matter

(2) Identifying cyber crime as a current community safety priority

(3) Recognizing that despite its complexity, cyber crime is actionable to some degree at all levels of policing; and,

WHEREAS the experience of other countries, combined with emerging domestic analysis, confirmed that the patterns of victimization, growing harm to communities, and threats to the rule of law, all fueled further by continued and rapid technological advances, argue urgently for a deliberate, coherent and sustained response by police services at all levels in Canada.

WHEREAS the CACP and its members, through adoption of this resolution, acknowledge that all "cybercrime", regardless of its underlying motivations, sources or forms, is in fact a crime; and, like all crime, it creates victims who merit our support. Notwithstanding the complexity and the need for broad collaborative strategies that must extend national capacity well beyond policing alone, **all levels of police agencies continue to bear an obligation, to the extent of their capacity, to prevent cyber-crime, to pursue cyber criminals and to protect their communities;**

THEREFORE BE IT RESOLVED…

That the Canadian Association of Chiefs of Police calls on its partners, their associations, and FPT stakeholders to work with the CACP to accelerate the advancement and adoption of a consolidated National Cyber Crime Strategy, as envisioned in Resolution #03-2012, including frameworks, mechanisms and a structure to achieve better national coordination within law enforcement, and among law enforcement, government, academia and the private sector;

BE IT FURTHER RESOLVED…

That the Canadian Association of Chiefs of Police calls on the Federal Government to increase focus on cybercrime in line with the principles above when it next updates "Canada's Cyber Security Strategy (2010);" and,

BE IT FURTHER RESOLVED…

That the Canadian Association of Chiefs of Police calls on its partners, their associations, and FPT stakeholders to collectively advocate for legislative, regulatory and policy change that will increase investigative efficiency and effectiveness, create greater risk and consequences for offenders, and more effectively facilitate the work of police in several areas, including but not limited to: reporting requirements; data preservation standards; MLAT reforms; domestic production orders for foreign data; modernized lawful access; and, extra- territoriality for certain vital cyber systems.