CANADIAN POLICE KNOWLEDGE NETWORK

RÉSEAU CANADIEN DU SAVOIR POLICIER

COMPETENCY-BASED MANAGEMENT FRAMEWORK FOR DIGITAL COMPETENCIES IN CANADIAN POLICING

A component of the Canadian Police Knowledge Network's *Cybercrime Training and Digital Competency Development for Canadian Law Enforcement* project

Paul Beesley, M.Sc. M.O.M.
Project Consultant

June 2021

The Cybercrime Training and Digital Competency Development for Canadian Law Enforcement project is funded, in part, by

Public Safety Canada
Sécurité publique Canada

Table of Contents

LIST OF TABLES

LIST OF FIGURES

Executive Summary

Using the Canadian Police Knowledge Network's Competency-based Management Framework this project has endeavoured to identify digital competencies for members of Canadian law enforcement as they relate to cybercrime, cyber-enabled crime, and digital evidence. Additionally, the report identifies readily available and accessible training that complements the competency profiles and makes recommendations for training development and capacity building.

A literature review identified current global practices for digital competencies. A series of focus groups involving over fifty police leaders, cybercrime experts, and cybercrime practitioners considered the digital competency framework established by the European Cybercrime Training and Education Group as a potential model for Canada. Ultimately, a Canadian version of a digital competency dictionary and competency profiles was created.

The Canadian framework defines ten digital competencies each consisting of five levels, namely:

1. Digital Literacy and the Internet
2. Cyber Hygiene and Cyber Security
3. Cybercrime Awareness, Prevention and Victim Assistance
4. Open-Source Intelligence and Evidence Gathering
5. Cyber Legalities
6. Cyber Data and Intelligence Analytics
7. Cryptocurrency and Blockchain
8. Programming and Scripting
9. Digital Forensics
10. Network Forensics

In addition, the framework identifies ten cyber-related roles in Canadian law enforcement agencies:

1. All Members of the Police Service (with access to computer networks and/or email systems)
2. First Responders
3. General Duties Investigators/Detectives
4. Intermediate Investigators (Cyber-related)
5. Outreach/Victim Liaison Professionals
6. Online Internet-based Investigators
7. Cybercrime Analysts
8. Digital Forensic Examiners
9. Cybercrime Investigators
10. Cyber Managers and Leaders

As outlined in Table 1, competency profiles that match competency levels with the various roles complete the competency aspect of the project.

Table 1. Digital Competency Profile Matrix for Canadian Law Enforcement

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
All Members	1	1								
First Responders*	1	2	2	1	1	1	1		2	1
General Detectives*	2	2	2	2	2	2	2		2	2
Intermediate Investigators*	3	3	3	2	2	2	2	3	3	3
Outreach Prevention/ Victim Assistance *	2	2	4	2	2	1	2		2	2
Open-Source Investigator*	4	3	2	4	3	3	3	3	2	3
Cybercrime Analyst*	3	3	2	3	2	4	4	4	2	3
Digital Forensic Examiner*	4	4	2	3	3	3	4	3	5	5
Cybercrime Investigator*	4	3	3	3	4	3	4	2	2	2
Leadership*	3	3	3	2	4	2	2		2	2

A training survey that followed the development of competency profiles identifies complementary training and informed a training gap analysis. The training gap analysis determined that while training for specialist roles such as Digital Forensic Examiner, Cybercrime Investigator, or Cybercrime Analyst is well established under the leadership of the Canadian Police College – Technical Crime Learning Institute there is substantial gaps in required training for generalist non-cyber roles such as First Responders and General Duties Investigators/Detectives. The gap analysis also recognized a need for additional training development in the areas of cyber victim assistance, cyber hygiene at lower levels, cyber legalities, cryptocurrencies, digital forensics at lower levels, and network forensics at lower levels.

RECOMMENDATIONS

There are nine 'next step' recommendations for digital competency capacity development:

1. Build training capacity for non-specialized cyber roles.
2. Build readily and easily accessible cyber hygiene training with a curriculum based on the All Members of the Police Service competency profile.
3. Rebuild CPKN's Cybercrime Investigations Level 1 course with a curriculum based on the First Responder competency profile.
4. Build readily and easily accessible cyber training with a curriculum based on the General Duties Investigators/Detectives competency profile.
5. Work with partners to build victim assistance modules with curricula based on competency Levels 1 and 2.
6. Work with partners to build or identify training in Cryptocurrency and Blockchain for law enforcement with competency Levels 1, 2, and 3 curricula.
7. Continue to liaise with the CACP E-Crimes Committee and the National Police Services Cybercrime Committee for annual review, evaluation, and validation of digital competency dictionary and profiles.
8. Continue evaluation of courses and cyber training to ensure they contain valid competency-based curricula.
9. Consider partnerships with public education institutions or private sector providers that are active in the cyber education space.

1. Project Overview

In early 2021, the Canadian Police Knowledge Network (CPKN) began an initiative to enhance digital competency-related training for Canadian law enforcement. Funded in part by Public Safety Canada's Cyber Security Cooperation Program, the *Cybercrime Training and Digital Competency Development for Canadian Law Enforcement* project engaged the Canadian policing community to apply a competency-based approach to:

1. Develop a digital competency dictionary for various roles and ranks within Canadian law enforcement agencies; and
2. Update/Develop bilingual training to enhance ability of frontline personnel to respond to cybercrime incidents.

1.1. The Competency-based Management Framework Approach

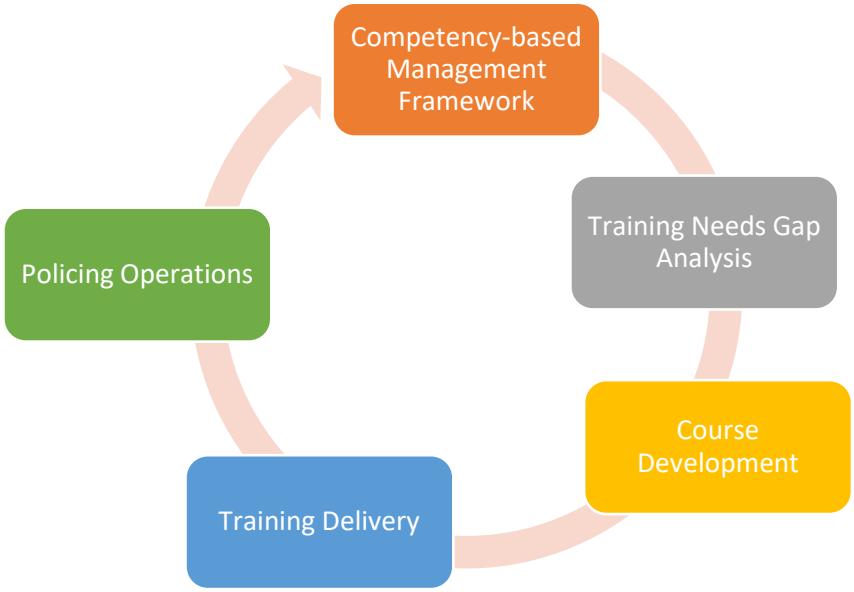
The Competency-based Management Framework (CBMF) centres on managing human resources by defining the skills, knowledge, and attributes that contribute to effective performance in a specific role. In a Canadian policing context, the CBMF classifies the core behavioural, technical, and leadership/ management competencies associated with general duty, investigative, and command roles (Canadian Police Knowledge Network, 2020, p. 1; Greenwood, 2020).

The development of a mature CBMF plays an essential role in:

- fulfilling the public's expectation that, regardless of province or community, all police are trained to a consistent and appropriate level of knowledge and skills;
- enabling police services to employ resources more effectively and efficiently;
- identifying gaps or deficiencies in policing performance and providing benchmarks by which police services can build capacity, improve decision making, and strategically adapt to the specific needs of their communities;
- ensuring officers have the skills and knowledge to effectively carry out their duties, including those difficult situations that often fall well outside the traditional boundaries of police work;
- providing measurable improvements in performance;
- decreasing organizational and officer risk, particularly in high-risk environments;
- improving employee morale and well-being (i.e., increase confidence, reduce workplace stress, and provide clear path for career advancement);
- strengthening overall policing and public safety outcomes;
- reducing the duplication of effort (and cost) among individual police services that are designing and employing Competency-Based Management models;
- improving transparency, accountability, and public trust in policing; and
- identifying opportunities to partner with social and health organizations to enhance the overall approach to community safety and well-being (Canadian Police Knowledge Network, 2020, p. 2).

As illustrated in Figure 1, the role-based digital competency framework allows for further analysis to identify training gaps, catalog existing training, and ultimately leads to the development and delivery of new training that ensures Canadian law enforcement agencies are better positioned to tackle the changing digital and cyber landscape.

Figure 1. Cyber Competency-based Management Framework



1.2. Methodology

This project included several phases to create a competency dictionary and make recommendations regarding the development and/or upgrading of existing training.

Phase 1: Review of Global Practice

A focused literature review was undertaken to provide a base for competency development and to create an understanding of global best practice. A focused literature review sought to define the term "cybercrime" and uncover existing digital competencies for law enforcement.

Phase 2: Consultation

Based on the literature review, a discussion paper, which consolidated global best practice, was written to frame focus group discussions.

The original plan envisioned various cyber subject matter experts and cybercrime investigative practitioners meeting for a multi-day workshop to define and develop a digital competency dictionary and digital competency profiles for Canadian law enforcement. The global pandemic and consequent travel restrictions, however, prevented the workshop from taking place. In its place, CPKN hosted a series of virtual focus groups with governance groups and practitioners from various law enforcement agencies.

Following the consultations, a roadmap existed for the development of a digital competency dictionary and digital competency profiles.

Phase 3: Creation of Competency Dictionary and Competency Profiles

The consultation phase provided the Canadian context to global best practice and identified both law enforcement cyber actors and competencies not previously identified.

The information and knowledge accumulated in the literature review, consultation phase, and development phase and were combined to create a draft of digital competencies for Canadian law enforcement. This included a competency dictionary describing the essential competencies through Levels 1 to 5 and competency profiles which identified the recommended competency levels for the various law enforcement cyber actors.

Phase 4: Training Survey and Gap Analysis

Upon completion of the competency profiles a survey of readily available and accessible training was undertaken. While not an exhaustive inventory of available training, the survey informs potential gaps in the training landscape and identifies opportunities for the creation of new or enhanced competency-based curriculum.

2. Review of Global Practice

2.1. Digital Crime, Cybercrime, or Just Crime?

When considering digital competencies, it is important to understand the context of their use. It might be a natural to think of digital competencies as being closely related to the skills police officers require to respond to cybercrime. However, the broad definition of cybercrime, coupled with exponential growth of digital evidence, might cause one to rethink the scope of digital competencies.

In Canada, there is no legal or single definition of what constitutes a cybercrime. Most of the country's law enforcement agencies use a definition developed by the Canadian Police College and adopted by the Canadian Centre for Justice Statistics and the Uniform Crime Reporting Survey (Mazowita & Vezina, 2014) where cybercrime is defined as:

> *"a criminal offence involving a computer as the object of a crime, or the tool used to commit a material component of the offence"* (Kowalski, 2002)

Cybercrimes are generally considered to have two distinct streams:

1. **Technology-as-Target** cybercrimes are offences where information technology, including devices and networks, are the target of the offence. Examples include unauthorized use of computer, denial-of-service attacks, and mischief relating to computer data.

2. **Technology-as-Instrument** cybercrimes offences are committed using information technology. These are often thought of as "traditional crimes", and examples include criminal harassment through social media or texting, distribution and sale of child pornography, and identity theft using information technology or the internet. (Ontario Provincial Police (2), 2016; Royal Canadian Mounted Police, 2021; Royal Canadian Mounted Police, 2015)

Figure 2. Cybercrime Categories

Source: (Royal Canadian Mounted Police, 2021)

Although there are nuances, there seems to be consistency in the multi-faceted approach to defining cybercrime around the world.

The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, defines cybercrime as a wide range of activities including the illegal interception and interference of data, computer-related offences such as fraud, and content-related offences such as the creation or distribution of child pornography [1] (Council of Europe, 2001). Europol differentiates cybercrime into cyber-dependent crimes and cyber-enabled crimes, where information and communications technology is the target in the former and where it is part of the offender's *modus operandi* in the latter. (Europol, 2018, p. 15)

The diverse nature of the cybercrime definition is exemplified in the Canadian experience. When compiling data on cyber-related violations Statistics Canada concludes that,

> "*The cybercrime violation represents the specific criminal violation within an incident in which a computer or the internet was the target of the crime, or the instrument used to commit the crime."* (Statistics Canada, 2021)

Table 2 illustrates that most cyber-related violations reported to Statistics Canada are generally considered as crimes in which technology is an instrument or part of the *modus operandi* of the offence; many of these incidents classified as cybercrimes are typically thought of as traditional crimes.

1. Canada is one of the sixty-five signatories of the Budapest Convention.

Table 2. Police-reported Cybercrime by Cyber-related Violation, Canada (selected police services)

Cyber-related Violation	2015	2016	2017	2018	2019
Total, all violations	**17,887**	**23,996**	**27,829**	**33,893**	**44,136**
Homicide	0	0	1	1	3
Invitation to sexual touching	109	77	101	104	118
Sexual exploitation	15	14	17	21	27
Luring a child via a computer	850	1,108	1,132	1,280	1,450
Voyeurism	67	58	80	77	88
Non-consensual distribution of intimate images	97	295	516	569	718
Extortion	709	797	893	1,863	1,410
Criminal harassment	1,001	1,058	1,291	1,396	1,715
Indecent/Harassing communications	1,202	1,655	2,302	2,708	4,933
Uttering threats	1,139	1,356	1,674	2,224	3,122
Other violent violations	69	149	195	251	300
Fraud	8,429	11,383	13,426	16,641	21,047
Identity theft	191	260	280	284	388
Identity fraud	695	828	1,082	1,369	1,920
Mischief	167	156	166	152	169
Other non-violent violations	8	27	66	181	270
Fail to comply with order	156	225	318	473	553
Indecent acts	10	19	23	20	35
Child pornography	1,753	1,278	1,041	621	1,130
Making or distribution of child pornography	850	2,886	2,868	3,113	4,174
Public morals	20	33	28	20	30
Breach of probation	39	68	74	98	120
Utter threats to property or animal	45	48	51	82	107
Offences against the person and reputation (Part VIII, *Criminal Code*)	110	89	82	142	118
Other *Criminal Code*	141	95	106	136	161
Other violations (Provincial Offences)	15	34	16	67	30

Source: (Statistics Canada, 2021)

Digital elements are becoming increasingly common across the spectrum of criminal offences. This experience is not uniquely Canadian. For instance, the Manhattan District Attorney's office noted that more that one-quarter of 2019 felony indictments in Manhattan involved a cyber component (Manhattan District Attorney's Office, 2021). Whereas the European Commission estimated that during the same period 85% of criminal investigations included some electronic evidence. (European Commission, 2019)

With Statistics Canada reporting that 91.3% of Canadians regularly use the internet, (Statistics Canada, 2021; Statistics Canada, 2019) and that over 80% of the population uses smart phones (Statistics Canada, 2021), it's hard to imagine a criminal act or so-called 'traditional crime' without potential for digital evidence. This sentiment is echoed by the Ontario Provincial Police that states,

> *"Every aspect of a police investigation is already affected by digital technologies in some way, and traditional models of processing digital evidence do not have the capacity to handle the volumes of digital evidence being seized as part of police investigations and to process them in a timely manner."* (Ontario Provincial Police (2), 2016, p. 3)

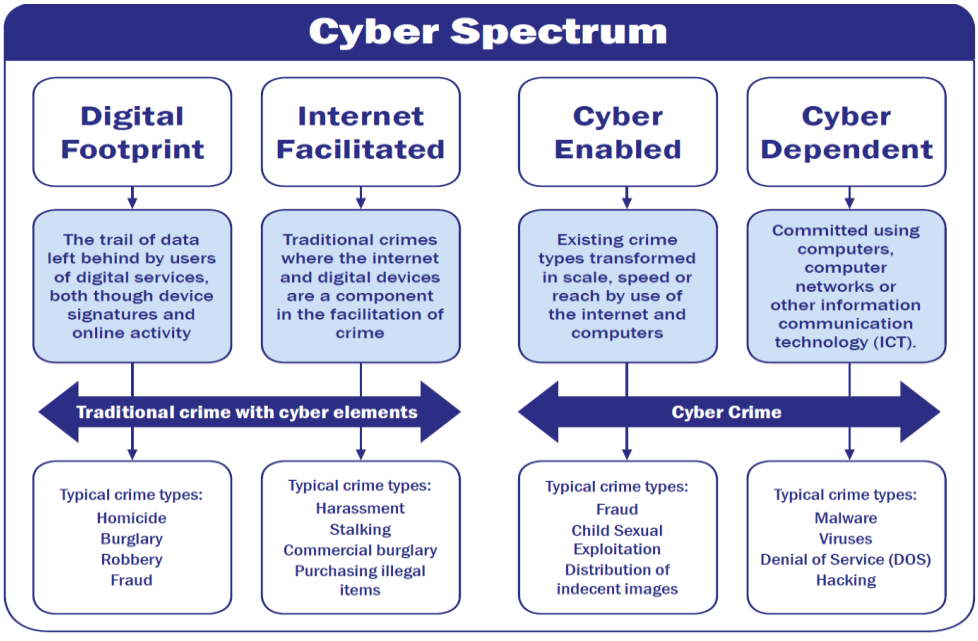
To further illustrate this point the United Kingdom's National Policing Digital Strategy recognizes that:

> *"The nature of "traditional" threats has evolved with digital platforms and technology. Almost every traditional crime now has a digital element to it in terms of both how it was committed, and how we can investigate it."* (Association of Police and Crime Commissioners, 2020, p. 4)

Digital competencies, it might be argued, need to extend beyond the already broad definition of cybercrime. The realities of policing and police response to cyber and digital elements requires an extended perspective of digital competencies. It requires a perspective that accounts for the expanding footprint of digital evidence that police officers are expected to understand and collect in a forensically sound manner.

The United Kingdom's Her Majesty's Inspectorate of Constabulary (HMCI) acknowledged that the scope of cyber and digital activity related to policing and crime has four distinct components: Digital Footprint, Internet Facilitated, Cyber Enabled and Cyber Dependent (Her Majesty's Inspectorate of Constabulary, 2015, p. 7). While HMCI refers to these components using the term "digital crime" the Lincolnshire Constabulary refined and illustrated the concept by coining the components of digital crime as the *cyber spectrum*.

Figure 3. The Cyber Spectrum of Crime



Source: (Lincolnshire Constabulary, 2021)

Though 'Internet Facilitated Crimes' are captured in the 'technology as an instrument' portion of the Canadian definition, the recognition of the 'Digital Footprint' as a component of the cyber spectrum is an important and necessary addition to building digital competencies. As observed by the Federal Bureau of Investigation,

> *"It's imperative that law enforcement agencies around the country—in particular, the first responders to a crime scene—have a working knowledge of how to survey and secure electronic evidence in addition to the physical evidence that they're more accustomed to, like fingerprints and DNA."* (Federal Bureau of Investigation, 2016)

2.2. The Division of Labour and Baseline Competencies

The CBMF strives to ensure that all Canadian law enforcement members are trained to a consistent and appropriate level of knowledge and skills. Clearly, a member of a police service engaged in a specialty area requires advanced competencies.

Advanced competencies build on a foundation of expected skills and knowledge. Consider, for instance, forensic identification. All police officers receive some training in forensic identification; they learn how to preserve evidence, the importance of the chain of continuity of evidence, etc. Some police officers receive additional training in crime scene examination where they might learn how to lift fingerprints and take crime scene photographs. Police officers engaged in the role of forensic identification officers receive highly specialized training in areas such as fingerprint analysis, photography, DNA collection, and blood pattern analysis. They are considered the experts in forensic identification techniques.

The same is true of digital competencies. Technology is reshaping crime as recognized by The Expert Panel on The Future of Canadian Policing Models,

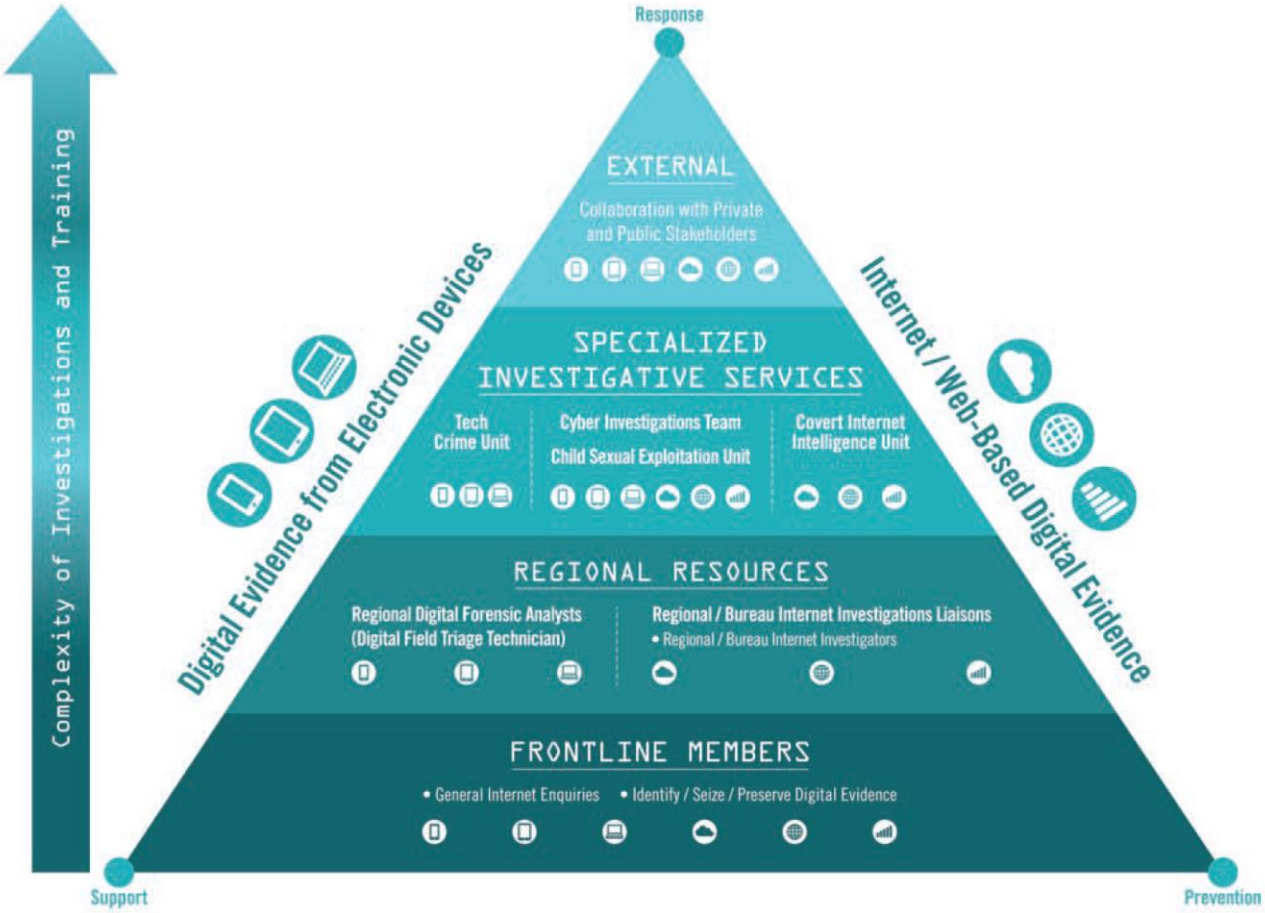
> *"Police services are increasingly responding to social problems for which they have limited training and resources. Demand is being influenced by an older, more diverse, and digitally savvy population."* (The Expert Panel on the Future of Canadian Policing Models, 2014, p. 14)

Given the ubiquity of digital evidence and the rise of technology enabled crimes, it is reasonable to expect that every member of a police service has a base level of digital competencies. Of course, persons specializing in digital forensic analysis or pure technology-on-technology crime are expected to acquire and maintain advanced competencies.

Although numerous Canadian law enforcement agencies operate units that specialize in things like digital forensics, child sexual exploitation, and technology-on-technology crime, it is estimated that less than 100 people are assigned to work exclusively in technology-on-technology cybercrime in Canada (Baron & Le Khac, 2021). As such, a tiered response to incidents with cyber or digital elements is becoming commonplace in Canadian policing (Royal Canadian Mounted Police, 2015; Ontario Provincial Police (2), 2016, p. 8; Kowalski, 2002).

The tiered response model, like the one developed by the Ontario Provincial Police (OPP) illustrated in Figure 4, identifies the roles members of police services play in response to incidents involving cyber or digital elements. The base represents foundational competencies required by all members of the service, while the peak represents activities and competencies beyond the service's capacity. As one moves up the pyramid, the volume of cyber-related occurrences decreases while the complexity of investigations increases. The complexity of investigations is matched by advanced competencies and training.

Figure 4. Tiered Digital Competencies by Role 1



Source: (Ontario Provincial Police (2), 2016)

An important aspect of the tiered response model is that it takes an enterprise-wide approach to digital- and cyber-related activity and the corollary competencies. It is unrealistic to expect a handful of highly-trained individuals to respond to every call for service that has a digital or cyber aspect.

To ensure police services can appropriately respond to the proliferation of digital evidence and cybercrimes—including high-volume crimes that leave a digital footprint or use technology as part of the *modus operandi*—the development of digital competencies that cover the entire cyber spectrum is essential. Multiple authors have identified the need for cyber knowledge across all roles within a policing organization (Robertson, 2019, p. 37).

The tiered response model implies that competencies are required on an enterprise-wide basis, starting with foundational competencies common to all members, and represent new opportunities for diversifying resources (The Expert Panel on the Future of Canadian Policing Models, 2014, p. 99). Empowering first responders to deal with crimes on the cyber spectrum by securing digital evidence, conducting preliminary investigative steps, and making appropriate referrals in more complex investigations is key to enhancing Canadian law enforcement's capacity in an increasingly digital world.

For example, consider a common scenario in which a police officer is dispatched to an assault which has been captured on social media. If the skills of a specialty unit were required to capture the digital evidence for all such calls, the specialty unit's workload would surely be unsustainable and detrimental to the investigation of more complex, time consuming, but less common pure cybercrime investigations for which the specialty unit is trained.

Although there is little or no data on the number of first responders trained in Canada to deal with issues across the so-called cyber spectrum, research suggests that the public expects police to respond to online crime and physical crime in a similar manner, that smaller police services are expected to respond to digital crime with the same level of service as larger agencies, and that those services that effectively dealt with the components of the cyber spectrum experienced greater public satisfaction (Robertson, 2019, p. 29).

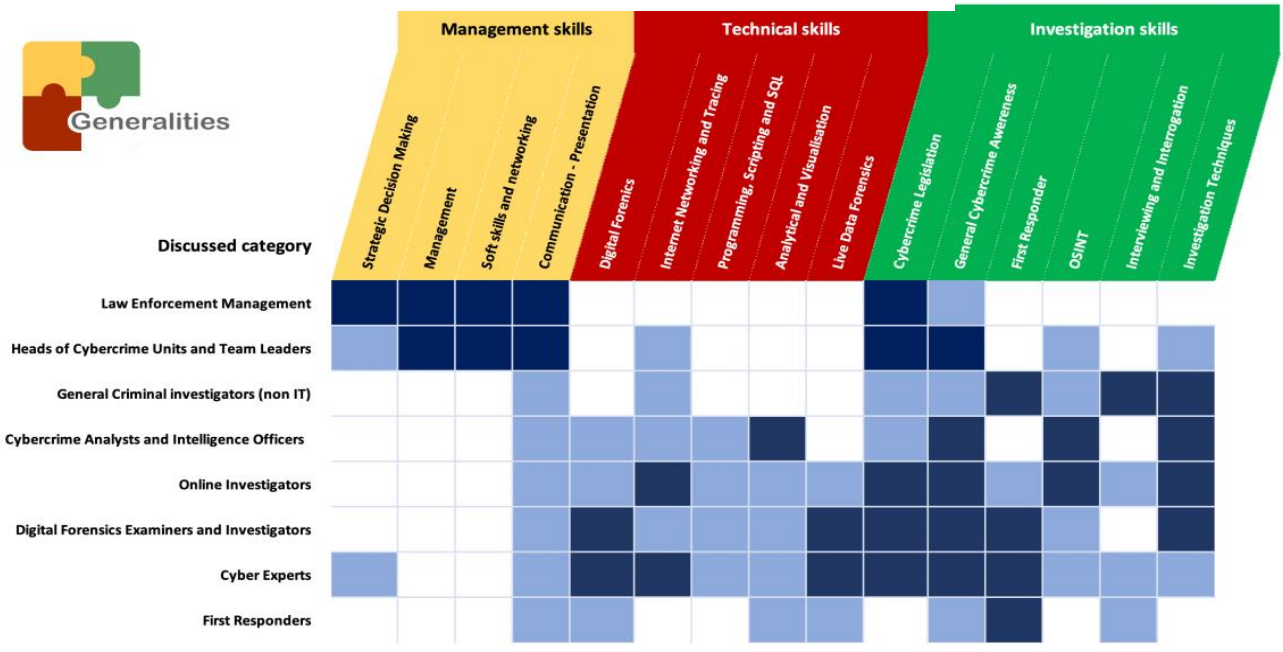
2.3. What Competencies Are Needed?

There are several international examples of digital competency development that may serve as a guide in the development of digital competencies for Canadian law enforcement.

The Budapest Convention on Cybercrime is the only binding international treaty on this issue. It serves as a guide for any country developing legislation against cybercrime and as a framework for international cooperation (The Council of Europe, 2020).

Flowing from the Budapest Convention and illustrated in Figure 5 [2], the European Union Agency for Law Enforcement Training, through its European Cybercrime Training and Education Group (ECTEG), created digital competencies for the various law enforcement 'actors' engaged in responding to crimes on the cyber spectrum (European Cybercrime Training and Education Group, 2020).

Figure 5. Matrix of Required Competencies for Law Enforcement Actors



Source: (European Cybercrime Training and Education Group, 2020)

[2] Light blue represents basic level training. Dark blue represents advanced level training.

The ECTEG matrix identifies law enforcement actors in terms of roles in a similar fashion to the tiered response model. It serves as a useful starting point in the development of a CBMF for most quadrants of the tiered response model. The ECTEG digital competencies are summarized in Table 3.

Table 3. Roles and Digital Competencies

Role	Description	Digital Competencies
Head of Cybercrime Unit/Team Leader	Deals directly with cyber investigators and experts. They should take informed decisions in cybercrime cases or in other complex investigations involving cybercrime elements.	• Profound knowledge of cybercrime and cybercrime offences • Advanced knowledge of legal and jurisdiction issues • Knowledge of the institutional framework for international cooperation • Knowledge of relevant investigating procedures • High-level knowledge of investigating and forensic tools • Knowledge of training needs and available resources • Staff management skills • Budget management skills • Project proposal drafting skills • Relationship management and soft skills • Communication skills
Cyber Experts	This category includes professionals involved as tactical law enforcement representatives in cyber attacks that cooperate with other actors (cyber security agency, CSIRT, related IT departments and management) in initiating coercive technical countermeasures, as well as acquiring, preserving, analyzing, and documenting complex (digital) traces and electronic evidence.	• Electronic evidence identification and seizing good practices • Advanced cybercrime awareness • Advanced network forensics • Strategic and operational cybercrime analysis • Analytical and visualisation tools • Scripting • Report drafting skills and evidence presentation • International judicial cooperation on cybercrime matters

Role	Description	Digital Competencies
Digital Forensic Examiner	These professionals perform detailed forensic examinations of computer based digital evidence.	• Advanced cybercrime awareness • Advanced knowledge of legal and jurisdiction issues • Processing of digital evidence while maintaining the chain of evidence • Expert knowledge in one or more forensic areas • Familiarity with different operating systems and applications • Knowledge of relevant commercial and open-source tools • Knowledge of scripting/programming and database querying (SQL) • Understanding of forensic artifacts and data carving • Knowledge of both *post-mortem* and live data forensics • Report drafting skills • Evidence presentation
Cybercrime Analyst	These professionals either focus on strategic analysis, researching, analyzing, and presenting the latest threats and providing situational overviews, or are more engaged in operational analysis to find patterns, trends, and hotspots and create links between live cases.	• Strategic and operational crime analysis • Big data management and analysis • Advanced cybercrime awareness • Analytical and visualisation tools • Open-source investigation • Social networks investigation • Scripting/programming • Network forensics • Report drafting skills • Evidence presentation • Fundamentals of undercover investigations
Online Investigator	These officers are tasked with monitoring the digital world and proposing new topics and cases to investigate, as well as carrying out or supporting the investigations.	• Advanced cybercrime awareness • Advanced knowledge of legal and jurisdiction issues • Processing of digital evidence while maintaining the chain of evidence • Advanced open-source investigation • Social networks investigation • Advanced network forensics • Report drafting skills • Undercover investigations • Scripting/programming • Interviewing skills • Evidence presentation

Role	Description	Digital Competencies
General Criminal Investigator	Mainstream investigators who are confronted with use of the internet and digital tools by criminals.	• Advanced cybercrime awareness • Advanced knowledge of legal and jurisdiction issues • Processing of digital evidence while maintaining the chain of evidence • Advanced open-source investigation • Social networks investigation • Advanced network forensics • Report drafting skills • Undercover investigations • Scripting/programming • Interviewing skills • Evidence presentation
First Responder	A first responder actor refers to law enforcement officers that are the first to get in contact with potential electronic evidence. Patrol police officers, detectives, border and tax controllers are all examples of first responders.	• Standards and best practices in electronic evidence identification and seizing • Basic live data forensics acquisition • Basic knowledge on digital forensics (tools, techniques, methods, and best practices), including internet technology, the dark web, and cryptocurrencies • Crime scene management • Interview techniques • General cybercrime awareness

Source: (European Cybercrime Training and Education Group, 2020)

In the United States, the National White Collar Crime Center (NW3C) has specialist certifications for cybercrime examiners and cybercrime investigators that specifically identify bodies of required knowledge (NW3C, 2021). The NW3C certification process, detailed in Table 4, may also be a useful guide in the development of advanced competencies for cyber spectrum policing activities.

Table 4. NW3C Cyber Certifications Body of Required Knowledge

Certified Cyber Crime Examiner (3CE)	Certified Cyber Crime Investigator (3CI)
Apply best practices in digital forensic techniques to image, document, and report on forensically sound digital evidence.	Detect, respond to, and investigate cybercrimes and crimes facilitated by online communication.
3CE Body of Knowledge:	3CI Body of Knowledge:
1. Technologies 2. Digital evidence handling 3. Forensic imaging 4. File system forensics 5. Forensic concepts 6. Legislative, legal, and regulatory framework	1. Theory and history 2. Common cybercrimes and internet-facilitated crimes 3. Collection and analysis of evidence held by Electronic Service Providers 4. Investigation of cybercrime and internet-facilitated crimes 5. Cyber security, cybercrime mitigation, and cyber hygiene 6. Legislative, legal, and regulatory framework

Source: (NW3C, 2021)

From an enterprise-wide perspective, Canadian research emphasizes the importance of cyber hygiene and digital literacy in police recruit training (Robertson, 2019, pp. 112-114).

Other Canadian-centric research (Baron & Le Khac, 2021) identified technical-, investigation-, and intelligence-related competencies for cybercrime investigators and digital forensic examiner specialists:

Technology

- Preservation and acquisition of malware, ICS-SCADA, VM, Encryption/Obfuscation/Steganography
- RAM analysis, database, backup, malware, ICS-SCADA, VM and Encryption/Obfuscation/Steganography
- Review of Digital evidence such as RAM, Database, Backup, etc.
- Review of Digital evidence such as malware, ICS-SCADA, VM and encryption/Obfuscation/Steganography
- Programming (SQL, Script, Java. Python, etc.)
- Network security concept, threats, vulnerabilities, impact, etc.
- Network investigation, incident response an intrusion detection
- Log analysis (Access, Firewall, IDS, IPS, etc.)
- Tools & Resources (Arcsight, Splunk, Wireshark, TDR, Netflow, etc.)
- Interception of live data capabilities
- Live data analysis 5.04 Malwares landscape

Investigation

- Testimony and Expert Testimony

Intelligence

- Cryptocurrencies
- Intelligence Resources & Tools
- Counterintelligence & Countermeasures

The importance of digital competencies for first responders, however, cannot be overstated as the tragic death of Rehtaeh Parsons highlighted,

> *"After the Rehtaeh Parsons case, there was an identified need for better education… Members in the front line just didn't know where to start."* (Thatcher, 2017, p. 17)

Although earlier versions of the ECTEG matrix overlooked digital competencies for first responders (Sobusial-Fischanaller & Vandermeer, 2016; European Cybercrime Training and Education Group, 2020), ECTEG has recently developed E-FIRST, the 'first responders learning package' through which it hopes to train thousands of first responders in the following digital competencies:

- Ability to identify and seize potential electronic evidence, including live data forensics
- Awareness of cybercrime, internet, encryption, dark web, and cryptocurrencies
- Assist victims of crimes facilitated by technologies when taking a complaint and starting a criminal case (European Cybercrime Training and Education Group, 2021)

A strong digital competency foundation for all members of the police service is also recognized as a key ingredient in the OPP's Cyber Strategy:

- The front line officer will have knowledge of and follow the OPP policy on dealing with digital evidence investigations
- Will be able to speak with members of the public in a professional and meaningful way on cybercrime issues
- Will have knowledge of the OPP's specialty services that can assist with cybercrime investigations and know how and when to contact them for further investigative assistance
- Will have knowledge of how to identify, seize, and protect the integrity of digital devices so they can be properly examined by OPP specialty services
- Will be responsible for creating the initial RMS Niche Report (including adding the property seized and scoring the appropriate UCR codes for a digital evidence investigation) and submitting a Request for Service form to the Technical Crime Unit
- The first point of contact for assistance with a digital device will be the Regional Digital Forensic Analyst, who will be able to provide advice to the officer on the appropriate level of specialty service required (Ontario Provincial Police (1), 2016, p. 16)

The need for first responder digital competencies and the lack of affordable training is recognized as an issue by the International Association of Chiefs of Police (IACP) (Federal Bureau of Investigation, 2016). In response, the IACP partnered with the FBI to launch an online program aimed at improving first responder's technical knowledge on how to survey and secure digital artifacts (Carnegie Mellon University, 2018).

The RCMP in British Columbia pioneered the development of Digital Field Triage to train first responder members to retrieve digital evidence, while RCMP members in Nova Scotia are trained to directly respond to cases with a cyber or technological element, including fraud, identity theft, online child exploitation, and cyberbullying (Siden, 2017; Thatcher, 2017).

While the first responder digital competencies in the latter initiatives are not explicitly defined, the notion and intent of enhancing first responders' ability to effectively respond to crimes with cyber and digital elements is consistent.

3. Consultation Phase

3.1. Focus Group Set Up

The original project plan envisioned various cyber subject matter experts and cybercrime investigative practitioners meeting for a multi-day workshop to define and develop a digital competency dictionary and digital competency profiles for Canadian law enforcement. However, the global pandemic and consequent travel restrictions prevented the workshop from taking place. Instead, CPKN hosted a series of virtual focus groups.

During March and April 2021, a series of two-hour virtual focus groups were held with industry and policing anti-cybercrime practitioners and experts from across Canada.[3] The focus groups included National Police Services Cybercrime Committee and the Canadian Association of Chiefs of Police E-Crimes Committee and its E-Crime Cyber Council sub-committee as the primary cybercrime governance groups.

A discussion paper based on the literature review served to consolidate global approaches to digital competencies in policing and frame the discussions with the focus groups. Focus group participants were provided with the discussion paper in advance of their session. The discussion paper asked readers to consider these questions:

1. Is there a need for digital competencies in policing?
2. If there is a need, should they be enterprise-wide or limited to specialized teams?
3. Is the CBMF the right approach to build digital competencies?
4. Is an expanded approach (beyond cybercrime) to digital competencies appropriate?
5. Is the tiered response model and division of labour an operationally viable model for Canadian policing?
6. Can we use the ECTEG model as a starting point?
7. Does your agency have digital competencies that can be shared?
8. What digital competencies are unique to the Canadian experience?
9. Are the digital competencies noted in the paper relevant to the Canadian experience?

3 Five sessions were held with a total of fifty participants from the following organizations: Calgary Police Service, Canadian Advance Technology Alliance, Canadian Police College, Canadian Police Knowledge Network, Edmonton Police Service, Microsoft Cybercrime Canada, Ontario Provincial Police, Ottawa Police Service, Public Safety Canada, RCMP – E Division, RCMP -Federal Policing, RCMP – K Division, Toronto Police Service, Saskatoon Police Service, Surete du Quebec, Society for Policing of Cyberspace and the Vancouver Police Department. There were fifty participants.

Additionally, focus group participants were provided joining instructions that provided them with context and information about the aims of the digital competency project. Included in the joining instructions were a set of draft competencies for discussion.

The joining instructions also asked participants to complete the following tasks prior to their focus group:

1. Please read the CPKN discussion paper. The paper is designed to frame the conversation and introduces concepts upon which we will rely during the focus groups.
2. Consider the roles identified in the discussion paper. Are they complete? Is there something missing? Are there identified roles that are not necessary?
3. Consider the draft competency profiles. Are they complete? Is there something missing? Are there identified roles that are not necessary?
4. Does your organization already have competency profiles for these or similar role? Can you share them with CPKN?

3.2. Focus Group Conclusions

Although the focus group discussion was organic, CPKN moderators captured the salient points regarding the above questions. Here are the key conclusions of the focus groups:

1. There was wide consensus regarding the need for additional cybercrime training for police officers and police professionals.
2. Training for cybercrime is required at all levels, from basic to advanced.
3. Many participants were unfamiliar with competency-based management frameworks.
4. There was agreement that competencies should inform training development.
5. Participants agreed that digital competencies should address technology-as-a-target crime, technology as an instrument to commit crime, and digital footprint evidence and that a broader definition of cybercrime was appropriate.
6. There was consensus that specialized cybercrime units do not have capacity to deal with high-volume cybercrimes such as internet-based fraud and digital footprint evidence. Most agencies in Canada have a formal or informal tiered response model already in operation.
7. There was recognition that most members of a police organization have exposure to activity on the cyber spectrum on a regular basis.
8. There was general agreement that generalists such as fist responders and detachment detectives should possess digital competencies but not necessarily at an advanced level.
9. Although the ECTEG model was seen as an interesting framework, there was not consensus on its adoption for the Canadian context. The primary reasons were that additional actors and additional competencies were required and the competency levels needed to be better defined.
10. None of the participants were able to provide existing digital competencies. The RCMP, OPP, Calgary Police Service, Saskatoon Police Service, and Vancouver Police Department were able to

provide job descriptions or training syllabi for specialized units in which competencies were implicitly included.

11. There was extensive discussion about the various roles in a law enforcement context. There was wide agreement on the specialized roles of digital forensic examiner, cybercrime investigators, and online open-source investigators.

12. Moderators directed the discussion to non-specialist roles and additional specialist roles. Most participants agreed that all members of the police service, first responders, generalist detectives and outreach/victim assistance were appropriate and necessary roles in the digital policing space.

13. Focus group participants independently identified the role of Intermediate Cyber Investigators like the RCMP's Digital Forensic Technician or the OPP's Regional Digital Forensic Analyst. Likewise, participants noted that the role of tactical and strategic intelligence analysts were vital to understand trends in cybercrime and identify persons of interest.

14. There was less agreement regarding the managerial and leadership role. Some police managers noted that because cybercrime was just a part of their portfolio it would be difficult to achieve the expertise level. Others pointed out that the role of managers and supervisors of dedicated cybercrime units should be included in the competency profile since managers are often assigned without prior experience in cybercrime.

15. There was wide-ranging discussion on the appropriate competencies. Although most participants agreed that the competencies identified in the ECTEG has general application in the Canadian context it was the consensus that the competencies needed to be better described and delineated by levels of competence.

16. Of the competencies included in the ECTEG model, the participants agreed that notwithstanding their concerns regarding description and delineation of competency levels that digital forensics, live data forensics, programming and scripting, data analytics, cybercrime awareness, and open-source intelligence were all competencies that are highly relevant in the Canadian context.

17. In addition to the relevant ECTEG competencies the themes of digital literacy, cyber hygiene, cyber security, cybercrime awareness, cybercrime prevention and cyber victim assistance were identified by various participants as essential competencies in the fight against cybercrime.

18. There was vigorous discussion on the changing and evolving law related to digital evidence and digital forensics. There was wide agreement that all members of police services should understand the case and statue law pertaining to digital evidence, including search and seizure and evidence presentation.

19. The rising importance and use of cryptocurrencies, coupled with a general lack of knowledge, was raised by participants on more than one occasion in more than one focus group. It was agreed that police officers needed at least an awareness of cryptocurrencies and their potential uses in criminal activities.

20. Because of the skill sets required and the potential ubiquity of Internet of Things devices, participants suggested that network (Cloud) forensics should be a competency that is distinct and separate from that of digital forensics.

4. Digital Competency Profiles

4.1. About Competencies

The primary component of the CPKN CBMF is a competency dictionary that details forty-two policing competencies. The competency dictionary breaks specialized investigative competencies into five levels (Canadian Police Knowledge Network, 2020). To ensure consistency with this approach, the predefined proficiency levels for investigative competencies will be used to build the digital policing competency profiles.

Table 5. Levels for Specialized Investigative Competencies CPKN Competency Dictionary

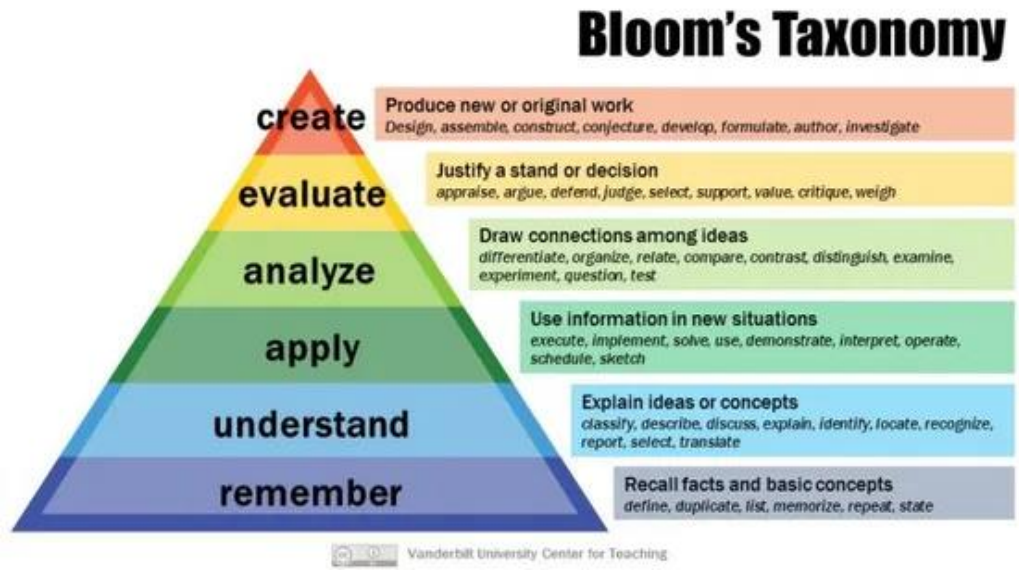
Level 1	Level 2	Level 3	Level 4	Level 5
Applies introductory knowledge in routine and predictable situations with guidance.	Applies basic knowledge in a range of typical situations that present limited challenges. Guidance required. Some individual autonomy or responsibility.	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance.	Applies advanced knowledge in a broad range of complex situations. Guides other professionals.	Applies advanced knowledge in most complex and unpredictable situations. Develops new approaches, methods or policies in the area. Provides guidance at a national and international level.

Source: (Canadian Police Knowledge Network, 2020)

Though the delineation of the five competency proficiency levels follows the framework used in the CPKN Competency Dictionary, the assignment of proficiency levels in the creation of the digital competency profiles is greatly informed by the revised Bloom's taxonomy. In simplified terms the competency proficiency levels are designed to equate to the six stages of the revised Bloom's taxonomy, as illustrated in Figure 6. [4]

[4] For more information on Bloom's Taxonomy (revised) see https://uwaterloo.ca/centre-for-teaching-excellence/teaching-resources/teaching-tips/planning-courses-and-assignments/course-design/blooms-taxonomy

Figure 6. Anderson and Krathwohl's (2001) Revision to Bloom's Cognitive Hierarchy



Source: (Armstrong, 2021)

Employment and Social Development Canada defines competencies as *"the combined utilization of personal abilities and attributes, skills and knowledge to effectively perform a job, role, function, task, or duty"* (Government of Canada, 2020). Competency attainment goes beyond attendance at courses. For instance, in addition to successful completion of the Technological Crime Learning Institute forensic program, the RCMP requires digital forensic examiners to complete a two-year understudy program (Baron & Le Khac, 2021, p. 15). The OPP has a similar understudy program for its digital forensic analysts.

At lower levels, however, competency attainment may be achieved though recall, awareness, and understanding (University of Waterloo, 2021). In these circumstances it is conceivable that a competency that requires proficiency at Levels 1 or 2 could be attained through education alone.

Broad competency headings and simplified descriptions like those used in the ECTEG matrix allow for competency 'evergreening'. For instance, if a competency with a broad heading like "Open-Source Intelligence and Evidence Gathering" captures the essence of the required knowledge and skills at each of the five proficiency levels, it avoids the need to continuously update and modify the competency as techniques and technologies evolve. This project aims to build competencies that are easy to understand and are enduring to inform competency-based training curricula. While a curriculum or training syllabus may need to be adjusted, the competency will remain valid or 'evergreen' regardless of changes in technology, investigative and forensic techniques, or law.

4.2. Competency Dictionary

Based on the responses of the focus groups, the review of global practices, and consideration of Bloom's taxonomy, a competency dictionary and digital competency profiles were formulated.

Ten digital competencies were identified as the required digital competencies for Canadian law enforcement:

1. **Digital Literacy and the Internet**
   The ability to find, evaluate, utilize, share, and create content using information technologies and the internet.
2. **Cyber Hygiene – Cyber Security**
   Practices and steps that users of computers and other devices take to maintain system health and improve online security.
3. **Cybercrime Awareness, Prevention, and Victim Assistance**
   Awareness of elements of the cyber spectrum (Digital Footprint, Internet Facilitated, Cyber Enabled, Cyber Dependent), prevention of victimization, and assistance to victims of cyber and cyber-enabled crime.
4. **Open-Source Intelligence and Evidence Gathering**
   Monitor and search known internet (social media sites, internet forums, weblogs, microblogs, podcasts, photographs or pictures, video, social bookmarking, etc.) to garner information to be shared as evidence or intelligence.
5. **Cyber Legalities**
   Legal issues that are unique to digital evidence including *Canadian Charter of Rights and Freedoms* considerations, case law, statute law, and international law, court presentation and prosecution readiness.
6. **Cyber Data and Intelligence Analytics**
   The examination of data sets to find trends and draw conclusions about the information they contain.
7. **Cryptocurrency and Blockchain**
   The use of cryptocurrency to buy goods and services, uses of online ledger cryptography to secure online transactions.
8. **Programming and Scripting**
   Designing and building an executable computer program to accomplish a specific computing result or to perform a specific task.
9. **Digital Forensics**
   Collection and analysis of digital media evidence to support investigations.
10. **Network (Cloud) Forensics**
    Analysis of networks and digital media evidence stored on networks to support investigation

A detailed description of each competency and the elements of each of the five levels is provided below.

Digital Literacy and the Internet				
The ability to find, evaluate, utilize, share, and create content using information technologies and the internet.		• Internet • Internet search tools • Use of common hardware and technology		
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Awareness of commonly used hardware and software Awareness of computer hardware operation Understands search, retrieve, and store data and information and content in digital environments Ability to interact through a variety of digital communication means including email for a given context Adheres to policies and procedures relevant to use of computers, digital devices, and networks	Understands computer peripheral devices and their operating procedures Awareness of common internet protocols Applies a variety of tools to search, retrieve, and store data and information and content in digital environments Uses common word processing and spread sheet software. Uses a variety of software to complete reports and presentations	Remains current with new and emerging technologies Provides guidance and advice on hardware and software applications that are commonly used in law enforcement context Knowledge of internet, intranets, e-commerce, e-business and converging technologies, network communication protocols, network architecture and topology, virtualized environment, handheld technologies, database and specialized test and monitoring software	Coaches and trains members of police service in areas of digital literacy Provides guidance on complex issues Gives advice on issues related to digital literacy in a law enforcement context Evaluates operating environment and provides strategic guidance to leadership Liaises with external agencies and other stakeholders	Creates tools, methods, and techniques for digital forensic analysis Provides expert advice on issues related to digital literacy in a law enforcement context at a national and international level Serves as a subject matter expert in the development and delivery of specialized training Serves as a subject matter expert in the development of legislation, regulations, or policies related to use of technologies

Seeks advice of subject matter experts when necessary	Uses various software to assist in investigations Understands digital footprints in an online environment Awareness of Virtual Private Network hardware and software, firewalls, Public Key Infrastructure applications	Understands and accesses online marketplaces including criminal marketplaces or those related to crime as a service Understands Dark Web, TOR criminal marketplaces, and trends	Identifies the need for research and development of new techniques and technologies Understands data communications protocols	Participates in professional associations Publishes research and white papers Presents at national and international conferences

Cyber Hygiene – Cyber Security				
Practices steps that users of computers and other devices take to maintain system health and improve online security.		• Passwords • Hardware • Phishing	• Malware • Digital Footprint • Digital Services "Privacy Policy"	
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Awareness of cyber hygiene and best practices for cyber security Awareness of social engineering and phishing as a potential target Awareness of techniques to protect devices and digital content Awareness of risks and threats in digital environments Awareness of corporate cybersecurity practices and policies including authorized hardware and software usage	Understands internet safety and privacy Awareness of the need to protect online identities Applies policies and protocols to protect personal and corporate information and cybersecurity Understands and applies techniques to deal with and limit personally identifying data produced through digital tools and environments Understands use of social engineering and commonly used phishing techniques	Remains current with emerging cyber security and emerging cyber threats Provides guidance to members of service on cyber hygiene and cybersecurity including reduction of digital footprint Understands network infrastructure technologies and components Applies cybersecurity principles by utilizing network monitoring technologies Applies techniques to create post exploitation attribution analysis	Understand the complex security environment including architecture, infrastructure, physical, identity and access management, and evolving technologies with involving multiple stakeholders Applies systems design, technology integration, and analysis techniques including testing methods and research and detailed reconnaissance practices Evaluates and recommends changes to corporate cybersecurity practices and policies	Creates new tools, methods, techniques for post attack digital forensic analysis Gives expert advice on issues related to cyber hygiene and cyber security in a law enforcement context at a national and international level Serves as a subject matter expert in the development of regulations, or policies related to cyber security and information security Participates in professional associations Publishes research and white papers

Understands concept of digital footprint in a law enforcement context Understands Password policies and password integrity Seeks advice of subject matter experts when necessary			Serves as a subject matter expert in the development and delivery of specialized training Uses industry common penetration testing tools and techniques to test cybersecurity	Presents at national and international conferences

Cybercrime Awareness, Prevention & Victim Assistance				
Awareness of elements of the cyber spectrum (Digital Footprint, Internet Facilitated, Cyber Enabled, Cyber Dependent), prevention of victimization, and assistance to victims of cybercrime and cyber-enabled crime		• Types of cybercrime • Target hardening • Cybercrime prevention		• Victims' services • Community orientation
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Recognizes the elements of the cyber spectrum (Digital Footprint, Internet Facilitated, Cyber Enabled, Cyber Dependent) Awareness of national cybercrime resources (CAFC, Senior Busters, NC3) Awareness of available victims' services Seeks advice of subject matter experts when necessary	Recognizes common cybercrimes and cyber-enabled crimes Understands information required when taking reports of cybercrimes and cyber-enabled crimes Understand and facilitates referral of victims of cybercrime and cyber-enabled crimes to appropriate victim services and resources Awareness of techniques to prevent cybercrime and cyber-enabled crime victimization	Understands technology-on-technology crime, cyber-enabled crime, and techniques used by offenders Provides guidance to police and community (individuals and corporate entities) on cybercrime and cyber-enabled crime prevention Understands and anticipates needs of victims of cybercrime and cyber-enabled crime Provides guidance regarding available services for victims of cybercrime and cyber-enabled crime	Evaluates emerging trends in cybercrime and cyber-enabled crimes and provides guidance on preventing victimization Evaluates operating environment and provides strategic guidance to leadership on matters related to cybercrime prevention and victim response/services Liaises with external agencies and other stakeholders to evaluate and create prevention programs and enhance cybercrime victim services	Gives expert advice on cybercrime prevention and victim services at a national and international level Serves as a subject matter expert in the creation and delivery of specialized training regarding cybercrime prevention and victims' services Serves as a subject matter expert in the development of legislation, regulations, or policies considerations regarding the delivery of cybercrime prevention programs and enhanced victims' services

		Understands peripheral victimology of cyber attacks on third-party entities	Liaises with public and private sector corporate cybersecurity and information security managers regarding cyberthreat landscape Provides training on cybercrime prevention and victims services	

Open-Source Intelligence and Evidence Gathering				
Monitor and search known internet (social media sites, internet forums, weblogs, microblogs, podcasts, photographs or pictures, video, social bookmarking, etc.) to garner information to be shared as evidence or intelligence		• Search engines • Meta crawlers • Dark web • Social media	• Geo location • Web monitoring • Chat P2P	
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Understands the term "open source" Uses common internet search engines Awareness of internet addresses, including internet navigation Uses common social media and marketplace sites Awareness of digital footprint Seeks advice of subject matter experts when necessary and understands how and where to seek advice	Understands the use internet as investigative research tool Understands the fundamental concepts of online research, investigation, and intelligence, including essential tools and techniques Understands digital footprint attribution profile and IP proxies Understands privacy and security issues related to open-source information gathering Awareness of dark web and TOR	Analysis of meta data Applies advanced internet search techniques including geolocation and geo fencing and de-anonymizing users in live and historical context Applies advanced search techniques and software to search dark web and TOR. Applies tools to preserve and ensure integrity of online sourced materials Understands law and policy in the creation and use of social media investigator non-covert and covert accounts and "honey-pots"	Coaches Evaluates emerging technologies and changes in law pertaining to open-source evidence and intelligence Evaluates and provides guidance on research and collection plans Evaluates and provides guidance on complex open-source issues and the use of investigator accounts and honey-pots	Gives expert advice on issues related to source evidence collection and intelligence at a national and international level Serves as a subject matter expert in the creation and delivery of specialized training Serves as a subject matter expert in the development of legislation, regulations, or policies considerations in the use of social media evidence and the creation of investigator non-covert and covert accounts and honey-pots

Understands law and policy in the use of open-source social media evidence Understands how to document internet searches and present in legal proceedings		Provides guidance and evaluates on open-source techniques, use of proxy accounts, privacy, and security considerations Uses and accesses online marketplaces including criminal marketplaces or those related to crime as a service Applies principles of sourcing in creation of reports Testifies	Evaluates operating environment and provides strategic guidance to leadership on matters related to open-source intelligence and evidence gathering Liaises with external agencies and other stakeholders Provides training on open-source evidence collection and intelligence Conducts peer review evaluation of reports and sourcing Ensures compliance with privacy and security policies and legislation	

Cyber Legalities				
Legal issues that are unique to digital evidence including Charter considerations, case law, statute law and international law. Court presentation and prosecution readiness		• Practical application of search and seizure law regarding data and digital devices • Evidence presentation • Evidence continuity • Reports and notes • Privacy and archiving • Treaties and access to international data		
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Awareness of privacy, freedom of information and archiving requirements and policies governing the use of computer networks and information retention Awareness of evidence management principles Applies ancillary powers for search and seizure of digital devices and digital evidence Understands documentation of actions related to digital evidence Understands articulation of legal authorities for actions	Understands chain of custody as it pertains to digital devices and digital evidence Applies principles of drafting judicial orders for investigations involving digital evidence Understands documentation and disclosure requirements regarding digital evidence. Understands how to present digital evidence in legal proceedings	Evaluates and provides guidance on search and seizure of digital devices, data, and other digital evidence Evaluates plans and provides guidance on reasonable expectation of privacy in digital devices and related data Applies techniques to prove authenticity and continuity of digital artifacts	Maintains currency on case and statute law pertaining to search and seizure of digital devices, data, and digital evidence Understands and maintains current knowledge of international treaties relating to digital evidence Liaises with external agencies and other stakeholders to ensure awareness of case and statue law as it pertains to digital evidence	Serves as a subject matter expert in the development of legislation, regulations, or policies considerations regarding search and seizure of digital devices and digital evidence Serves as a subject matter expert in the development of policies considerations regarding the role and involvement of digital evidence expert witnesses

Seeks advice of subject matter experts when necessary		Awareness of international treaties on digital evidence and their application to domestic investigations Understands jurisdictional issues and complexities related to trans-border movement of data and data stored on networks (cloud storage) Evaluates and provides guidance on drafting of complex judicial orders including MLAT and general warrants	Applies criteria relating to use of expert witnesses and provides opinion evidence as required Evaluates plans and provides guidance to case managers on the use and limitations of experts and expert witnesses in an investigation Creates and delivers training on judicial orders as they pertain to digital devices and digital evidence	

Cyber Data and Intelligence Analytics				
The examination of data sets to find trends and draw conclusions about the information they contain.		• Databases • Statistical analysis • Data science • Linkage analysis • Analytics software		
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Awareness of police databases and their application to issues on the cyber spectrum Seeks advice of subject matter experts when necessary	Understands issues associated with criminal activity related to the cyber spectrum Awareness linkage and other data analysis to support investigations Applies readily available tools to search databases for information Performs routine analysis of data sets	Evaluates emerging trends and criminal activity of the cyber spectrum Produces strategic intelligence reports relating emerging cybercrime and emerging trends Uses appropriate software to interrogate data to assist ongoing investigations by creating linkage charts Produces tactical and operational reports related to data analysis Applies appropriate data analysis techniques and software applications	Coaches Applies principles of data science including statistical analysis to produce strategic reports Provides advice on data management and the use of statistical analysis and recommends use of appropriate software Evaluates and provides guidance on analytical techniques Liaises with external agencies and stakeholders on data analytics related to criminal activity on the cyber spectrum	Creates new tools, methods, techniques for embedded and stand-alone executables Gives expert advice on issues of data analysis relating to cybercrime and emerging trends at a national and international level Serves as a subject matter expert in the development of data analysis related to law enforcement issues of the digital spectrum Participates in professional associations Publishes research and white papers

		Integrates intelligence analysis principles with industry-standard frameworks for the assessment of cyber threats and threat actors Testifies	Identifies and evaluates threats and actors engaged in criminal activity on the cyber spectrum Creates threat assessments Identifies and evaluates avenues to infiltrate, investigate detect, prevent, deter and/or disrupt cyber criminal networks Applies concepts associated to Big Data analysis and associated software	Presents at national and international conferences

Cryptocurrency & Blockchain				
The use of cryptocurrency to buy goods and services, uses of online ledger cryptography to secure online transactions.		• Various currencies • Wallets • Blockchain	• Distributed networks • QR codes • Mining	
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Awareness of cryptocurrencies Awareness of anonymity of cryptocurrency transactions Seeks advice of subject matter experts when necessary	Understands fundamentals of how cryptocurrencies work Awareness of cryptocurrency transaction mechanisms including Bitcoin addresses Understands how and where cryptocurrencies are converted into hard currency Understands signs of cryptocurrency including QR codes and digital wallets Awareness of distributed networks and blockchain	Applies key vocabulary and concepts related to blockchain and cryptocurrencies Understands criminal use of cryptocurrency Understands how to acquire, dispose of, and recover various cryptocurrencies Uses cryptocurrency Uses and applies security best practices for cryptowallets in a law enforcement context Applies techniques to trace cryptowallets	Understands structure, uses, and applications of blockchain technology Understands use of blockchain beyond cryptocurrency Liaises with external agencies and stakeholders on issues related to cryptocurrency in a law enforcement context Identifies and evaluates emerging issues related to cryptocurrency and blockchain in a law enforcement context Evaluates operating environment and provides strategic guidance to leadership	Creates new tools, methods, techniques for forensic analysis of cryptocurrencies and block chain technologies Gives expert advice on issues related to cryptocurrencies in a law enforcement context Serves as a subject matter expert in the creation and delivery of specialized training Serves as a subject matter expert in the development of legislation, regulations, or policies relating to cryptocurrencies and block chain Participates in professional associations

		Applies storage and security requirements of cryptocurrency Evaluates and provides guidance on seizure and storage of cryptocurrency Testifies	Understands legislation and regulations pertaining to cryptocurrencies and blockchain Creates and delivers training on cryptocurrency and blockchain in a law enforcement context	Publishes research and white papers Presents at national and international conferences

Programming and Scripting				
Designing and building an executable computer program to accomplish a specific computing result or to perform a specific task.		• Programming languages • Coding skills • SQL • Boolean operators		
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Awareness of coding and scripting as the primary means of customizing software and effectively searching data Uses graphical interface search tools Seeks advice of subject matter experts when necessary	Uses Boolean operators in search engines; may seek advice on syntax and order of operations Uses pre-written code, scripts, and SQL commands as stand-alone executables or as macros within software and understands their operations	Uses one or more programming and scripting languages without guidance to build basic stand-alone and embedded executables Reads code and interprets function of program, including error debugging Provides guidance on Boolean and SQL Provides guidance on the appropriate uses for embedded script	Conducts in-depth analysis of code and scripts Uses various computer languages and scripts to build complex stand-alone and embedded executables Coaches on the fundamentals of script writing or coding Liaises with external agencies and stakeholders on customized software solutions related to law enforcement issues on the digital spectrum	Creates new tools, methods, and techniques for embedded and stand-alone executables Gives expert advice on issues related to scripting and coding related to law enforcement activities of the digital spectrum at a national and international level Serves as a subject matter expert in the development of investigation and enforcement related software

			Identifies and evaluates appropriate coding languages and solutions for software development related to law enforcement activities on the digital spectrum	Serves as a subject matter expert in the development of software related to law enforcement issues of the digital spectrum Participates in professional associations Publishes research and white papers Presents at national and international conferences

Digital Forensics				
Collection and analysis of digital media evidence to support investigations.		• Dead data forensics • Live data forensics • Operating systems	• Networks • Encryption and obfuscation	
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Understands potential sources of digital evidence Understands need to preserve and value of digital evidence Adheres to service's policies and procedures relevant to search, seizure, and handling of digital evidence Seeks advice of subject matter experts when necessary	Understands digital media storage, including: - computer - cell phone - internet - camera Understands potential digital evidence related to common cybercrime and cyber-enabled crimes including: - malware - spam - fraud - identity theft - cyber bullying - child exploitation - sexting Uses basic forensic tools to collect readily obtainable digital evidence	Keeps current with emerging technologies Evaluates investigative plans and provides guidance to front line members and investigators Identifies and evaluates forensic artifact evidence Provides on-site support during an execution of search warrants Applies forensic principles in the acquisition, preservation, and examination of dead and live digital evidence	Coaches Provides guidance on complex issues Evaluates operating environment and provides strategic guidance to leadership Liaises with external agencies and other stakeholders Evaluates and conducts complex network investigations Conducts peer review evaluation of digital evidence for legal admissibility in criminal cases	Creates new tools, methods, techniques for digital forensic analysis Gives expert advice on issues related to digital forensic analysis at a national and international level Serves as a subject matter expert in the development and delivery of specialized training Serves as a subject matter expert in the development of legislation, regulations, or policies in digital forensic analysis Participates in professional associations

	Understands legislation relevant to search, seizure, and handling of digital evidence Understands how to document and present digital evidence Awareness of commonly used encryption protocols and signs of encryption	Understands typical de-obfuscation and tracing techniques Understands file systems and major distinguishing features of operating systems Uses common encryption protocols and un-encryption techniques Testifies as expert	Identifies and evaluates the need for research and development of new techniques and technologies Understands legislation pertaining to digital forensic analysis Manages the acquisition of tools for digital media analysis	Publishes research and white papers Presents at national and international conferences

Network Forensics				
Analysis of networks and digital media evidence stored on networks to support investigations.		• Network architecture • Network tracing • Cloud • Encryption and obfuscation		
Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Applies introductory knowledge in routine and predictable situations with guidance	Applies basic knowledge in a range of typical situations that present limited challenges; guidance required; some individual autonomy or responsibility	Applies solid knowledge in a full range of non-typical situations of moderate complexity with minimal guidance or no guidance	Applies advanced knowledge in a broad range of complex situations; guides other professionals	Applies advanced knowledge in most complex and unpredictable situations; develops new approaches, methods, or policies in the area; provides guidance at a national and international level
Awareness of networks and Cloud as a user Understands legislation relevant to search, seizure, and handling of digital evidence obtained from cloud storage other remote networks Adheres to service's policies and procedures relevant to search, seizure, and handling of digital evidence obtained from cloud or other remote networks Seeks advice of subject matter experts when necessary	Understands fundamentals of computer networking components, hardware, and packets Awareness of types of network addresses, TCP and UDP protocols, email forward and reverse lookup possibilities Awareness of typically available evidence from network (Cloud) digital footprint Awareness of digital artifacts (Passwords, QR codes, PKI Keys) that provide access to cloud storage or remote network storage	Keeps current with new and emerging network technologies Evaluates plans and provides guidance to front line members and investigators re cloud and networks Provides on-site support during an execution of search warrants Applies forensic techniques to locate, acquire, preserve, and examine digital evidence stored at remote networks or data centres Applies forensic techniques to identify artifacts that assist with identity and access management	Coaches Provides analysis and evaluation of network architecture Provides guidance on complex issues involving network architecture and their forensic analysis Evaluates operating environment and provides strategic guidance to leadership Liaises with external agencies and other stakeholders Evaluates incident response options and oversees incident response	Develops new tools, methods, techniques for network forensic analysis Gives expert advice on issues related to network forensics at a national and international level Serves as a subject matter expert in the development and delivery of specialized training Serves as a subject matter expert in the development of legislation, regulations, or policies in digital forensic analysis Participates in professional associations

		Applies forensic principles to de-obfuscation and network tracing Applies principles of cryptography and un-encryption techniques Authors technical forensic reports for court Testifies	Evaluates proposed forensic network investigations Identifies the need for research and development of new techniques and technologies Possesses an in-depth understanding of legislation pertaining to digital forensic analysis of networks including trans-border movement of data Manages the acquisition of tools for network analysis Provides expert testimony	Publishes research and white papers Presents at national and international conferences

4.3. Cyber Actors

Complementary to the digital competencies, these ten cyber actors or roles were identified as those that are regularly engaged in law enforcement take activities on the cyber spectrum:

All Members of the Police Service

Every employee or volunteer of a police service with access to the computer network. These competencies serve as a competency baseline for all other roles.

First Responders

Members of police services who respond to calls for service. They are typically the first persons to respond to criminal activity and work in uniform. These competencies also serve as a foundation for all other roles.

General Duties Investigators/Detectives

Police investigators who primarily work in general investigation sections, criminal investigation bureaus, crime units, or divisional detective offices. They are typically community-based and deal with the investigation of criminal activity beyond the capacity of uniform first responders.

Cyber-related Intermediate Technicians

Police professionals with extra capacity and training to seize electronic evidence and support investigations that have digital elements, including basic data extraction, data capture, and data seizure. They provide local advice and assistance on interviewing and judicial orders for investigations with digital elements. They prepare exhibits that require more advanced or technical examination and liaise with actors with advanced or expert knowledge.

Outreach and Victim Liaison Professionals

Police professionals who are engaged in providing their community with crime prevention advice. This group may include community service officers, school liaison officers, and victim liaison officers. Advanced level duties may include delivery of cyber security awareness, prevention, and education programs to industry, business, and government (e.g., municipalities, school boards, etc.).

Online Internet-based Investigators (OSINT)

Police investigators who conduct investigations primarily through the internet. They may include specialized investigators engaged in counter exploitation roles (CSE and human trafficking), national security investigators, and criminal intelligence officers. They monitor the internet as sort of 'digital patrol' officers. They identify and propose new investigations, and they are trained in OSINT techniques and technical areas such as tracing, obfuscation, encryption, and counter-forensics.

Cybercrime Analysts (Tactical and Strategic)

Police professionals engaged in strategic analyses to identify and research the latest cybercrime threats and activities or provide tactical support to ongoing investigations by identifying patterns, hotspots, and linkages in criminal activity. Persons engaged in this role need to be able to process large amounts of diverse data to produce concise and actionable reports.

Digital Forensic Examiners

Police professionals who perform expert forensic examinations regarding data at rest and retrieve digital artifacts from various hardware and networks.

Cybercrime Investigators

Police professionals who investigate and mitigate cyber attacks, including but not limited to DOS, data intrusion, and ransomware extortions; they acquire and preserve electronic

evidence, including tracing, and overcome obfuscation of origin.

Managerial and Leadership

Police professionals who deal with complex cybercrime investigations in a leadership capacity. They advise senior management on strategic initiatives and trends related to cybercrime, oversee operational aspects of their unit, and provide advice to other areas of the police service regarding cybercrime and/or digital evidence.

4.4. Digital Competency Profiles

The digital competency profile outlines which competencies and at which proficiency level the various cyber actors need to complete the essential elements of their jobs. The competency profiles are summarized in Table 6 followed by detailed description for each of the cyber actor's competency profiles.[5]

Table 6: Digital Competency Profile Matrix for Canadian Law Enforcement
** Additional non-digital competencies also recommended – see detailed profiles*

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
All Members	1	1								
First Responders*	1	2	2	1	1	1	1		2	1
General Detectives*	2	2	2	2	2	2	2		2	2
Intermediate Investigators *	3	3	3	2	2	2	2	3	3	3
Outreach Prevention/ Victim Assistance *	2	2	4	2	2	1	2		2	2
Open-Source Investigator*	4	3	2	4	3	3	3	3	2	3
Cybercrime Analyst*	3	3	2	3	2	4	4	4	2	3

[5] The profiles also include some non-digital competencies that are part of the existing CPKN-CBMF competency dictionary.

Digital Forensic Examiner*	4	4	2	3	3	3	4	3	5	5
Cybercrime Investigator*	4	3	3	3	4	3	4	2	2	2
Leadership*	3	3	3	2	4	2	2		2	2

All Members of Police Service that have Access to Computer Networks and/or Email Systems			
Description of Role	**Essential Training Requirements**	**Digital Competency**	**Level**
Every employee or volunteer of a police service with access to the computer network. These competencies serve as a competency baseline for all other roles.	Fundamental digital literacy Fundamental cyber hygiene Fundamental personal and organizational cyber security Fundamental privacy and archiving legislation and policy Where and how to seek assistance of specialized resources	Digital Literacy and the Internet Cyber Hygiene and Security	1 1

First Responders (Typically Uniform Patrol)			
Description of Role	**Essential Training Requirements** ***All Members of Police Service PLUS:***	**Digital Competency**	**Level**
Members of police services who respond to calls for service. They are typically the first persons to respond to criminal activity and work in uniform. These competencies also serve as a foundation for all other roles.	Fundamental digital literacy Identification of electronic evidence Digital forensics awareness Seizure and preservation of digital devices prior to forensic examination Informed consent for evidence collection Fundamental web capture techniques Fundamental digital evidence collection Fundamental digital crime scene management General cybercrime and cyber-enabled crime awareness Fundamental personal and organizational cyber security Victims' needs and available services Court presentation of digital evidence Cryptocurrency awareness Where and how to seek assistance of specialized resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Digital Forensics Network (Cloud) Forensics *Existing CPKN non-digital competencies:* • *Court Testimony* • *Crime Scene Management* • *Interviewing* • *Note Taking*	1 2 2 1 1 1 1 2 1

General Duties Investigators/Detectives			
Description of Role	**Essential Training Requirements** ***First Responders PLUS:***	**Digital Competency**	**Level**
Police investigators who primarily work in general investigation sections, criminal investigation bureaus, crime units, or divisional detective offices. They are typically community-based and deal with the investigation of criminal activity beyond the capacity of uniform first responders.	Fundamental cyber Investigation techniques Cybercrime and cyber-enabled crime awareness Fundamentals of evidence available from digital footprints Legal authorities, requirements, and procedures Fundamentals of open-source evidence and intelligence gathering Fundamentals of social networks investigation Fundamentals of cryptocurrency Victims' needs and available services Interviewing Where and how to seek assistance of specialized resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Court Testimony* • *Crime Scene Management* • *Interviewing* • *Obtaining Judicial Authorizations* • *Note Taking*	2 2 2 2 2 2 2 2 2

Cyber-related Intermediate Technicians			
Description of Role	**Essential Training Requirements**	**Digital Competency**	**Level**
Police professionals with extra capacity and training to seize electronic evidence and support investigations that have digital elements including basic data extraction, data capture, and data seizure. They provide local advice and assistance on interviewing and judicial orders for investigations with digital elements. They prepare exhibits that require more advanced or technical examination and liaise with actors with advanced or expert knowledge.	Advanced cybercrime and cyber-enabled crime awareness Advanced knowledge in area of specialization (mobile devices, computer, networks) Practical application of digital crime scene management principles Practical application of network and IP tracing principles Scripting and coding Legal authorities, requirements and procedures Technical and forensic report writing Technical and forensic testimony Practical application of cryptocurrency Where and how to seek assistance of specialized or expert resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Programming and Scripting Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Court Testimony* • *Crime Scene Management* • *Note Taking*	3 3 3 2 2 2 3 3 3

Outreach/Victim Liaison Professionals			
Description of Role	**Essential Training Requirements**	**Digital Competency**	**Level**
Police professionals engaged in providing their community with crime prevention advice. This group may include community service officers, school liaison officers, and victim liaison officers. At advanced level duties may include delivery of cyber security awareness, prevention, and education programs to industry, business, and government (e.g., municipalities, school boards, etc.).	Advanced cybercrime and cyber-enabled crime awareness High-volume cybercrime prevention techniques Advanced cyber hygiene Victims' needs and available services Community mobilization models Prevention of cybercrime resource and network development Practical application of cryptocurrency Crime as a Service (CaaS) and criminal marketplaces Where and how to seek assistance of specialized or expert resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Interviewing (Victims)* • *Note Taking* • *Fostering Partnerships* • *Community Relations and Media Management*	2 2 3/4 2 2 1 2 2 2

Online Internet-based Investigators (OSINT)			
Description of Role	**Essential Training Requirements**	**Digital Competency**	**Level**
Police investigators who conduct investigations primarily through the internet. This may include specialized investigators engaged in counter exploitation roles (CSE and human trafficking), national security investigators, and criminal intelligence officers. They monitor the digital as sort of 'digital patrol' officers. They identify and propose new investigations and are trained in OSINT techniques, technical areas such as tracing, obfuscation, encryption, and counter-forensics.	Advanced cybercrime and cyber-enabled crime awareness Legal authorities, requirements, and procedures Programming and scripting Advanced open-source investigation Advanced internet search techniques Social networks investigation dark web, TOR, online criminal markets and Crime as a Service (CaaS) Advanced online de-obfuscation Network forensics Cryptocurrency practical application Technical and forensic report writing Fundamentals of online undercover operations Expert evidence presentation Where and how to seek assistance of specialized or expert resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Programming and Scripting Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Court Testimony* • *Crime Scene Management* • *Note Taking* • *Criminal Intelligence Analyst*	3/4 3 1 4 3 3 3 2/3 2 2/3

Cybercrime Analysts (Tactical and Strategic)			
Description of Role	**Essential Training Requirements**	**Digital Competency**	**Level**
Police professionals engaged in strategic analysis to identify and research the latest cybercrime threats and activities or provide tactical support to ongoing investigations by identifying patterns, hotspots, and linkages in criminal activity. Persons engaged in this role need to be able to process large amounts of diverse data to produce concise and actionable reports.	Strategic and tactical crime analysis Big data analytics Statistical analysis Advanced cybercrime and cyber-enabled crime awareness Open-source investigation Social networks Network forensics Scripting and coding Evidence presentation Cryptocurrency Dark web, TOR, online criminal markets and Crime as a Service (CaaS) Technical and forensic report writing Expert evidence presentation Where and how to seek assistance of specialized or expert resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Programming and Scripting Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Court Testimony* • *Crime Scene Management* • *Note Taking* • *Criminal Intelligence Analyst*	3 3 2 3 2 4 3/4 2/3 2 3

Digital Forensics Examiner			
Description of Role	**Essential Training Requirement** ***Intermediate and Advanced Investigators PLUS:***	**Digital Competency**	**Level**
Police professionals who perform expert forensic examinations regarding data at rest and retrieve digital artifacts from various hardware and networks.	Advanced digital and hardware literacy Advanced cybercrime and cyber-enabled crime awareness Expertise in area of forensic specialization (mobile devices, computer, network) Legal authorities, requirements, and procedures related to digital evidence Technical and forensic report writing Advanced operating systems and applications Advanced de-obfuscation and encryption Advanced knowledge of forensic artifacts and data carving Advanced cryptocurrencies Expert evidence presentation, including understanding role and limitations of expert witnesses Where and how to seek assistance of specialized or expert resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Programming and Scripting Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Court Testimony* • *Crime Scene Management* • *Interviewing* • *Obtaining Judicial Authorizations* • *Note Taking*	4 4 2 3 3 3 3/4 3 4/5 4/5

Cybercrime Investigator			
Description of Role	**Essential Training Requirements** ***General Duties Investigator PLUS:***	**Digital Competency**	**Level**
Police professionals who investigate and mitigate cyber attacks including but not limited to DOS, data intrusion, and ransomware extortions. They acquire and preserve electronic evidence, including tracing, and overcome origin obfuscation.	Advanced cybercrime threat awareness Advanced cybercrime and cyber-enabled crime awareness Network and digital forensics Scripting and coding Advanced Cryptocurrencies Technical and forensic report writing Interviewing skills Legal authorities, requirements, and procedures Expert evidence presentation Where and how to seek assistance of specialized or expert resources	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Programming and Scripting Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Court Testimony* • *Crime Scene Management* • *Interviewing* • *Obtaining Judicial Authorizations* • *Note Taking*	4 3 3 3 3/4 2/3 3/4 2 2 2

Managerial and Leadership			
Description of Role	**Essential Training Requirements**	**Digital Competency**	**Level**
Police professionals who deal with complex cybercrime investigations in a leadership capacity. They advise senior management on strategic initiatives and trends related to cybercrime, oversee operational aspects of their unit, and provide advice to other areas of the police service regarding cybercrime and or digital evidence.	High-level cybercrime and cyber-enabled crime awareness Legal authorities, requirements, and procedures Fundamentals of cybercrime investigative techniques Victims' needs and available services Technology change management and quality management skills Financial management – budgeting, procurement of technology Incident management Project management principles Human resource management of technical professionals Change management Information technology management Strategic Management	Digital Literacy and the Internet Cyber Hygiene and Security Cybercrime, Prevention, and Victim Assistance Open Source Cyber Legalities Data and Intelligence Analytics Cryptocurrency and Blockchain Digital Forensics Network (Cloud) Forensics *Existing CPKN-CBMF non-digital competencies:* • *Performance Competencies* • *Partnering Competencies* • *Accountability Competencies*	3 3 3-4 2 3-4 2 2 2 2

5. The State of Currently Available Training in Canada

5.1. Training Survey

An open-source survey to identify training that matches the competency profiles followed the development of the digital competency profiles. The training survey serves only to provide examples of currently available cyber training. The following limitations apply to the training survey:

1. The survey considers only readily available training (i.e., training that any Canadian law enforcement agency may quickly identify and be able to enroll their members). It does not include training that has been developed "in-house" that is not advertised or easily accessible by the broader Canadian law enforcement community.

2. The survey is based on open-source searches of the internet and is not meant to be exhaustive or complete. It provides only examples of readily available training.

3. It does not consider tuition fees, travel expenses, or provide an assessment of value for money.

Despite these limitations the training survey provides an overview of training that Canadian chiefs of police or training sections can easily access to fulfill some or all the training requirements that complement the competency profiles. It also provides some guidance on themes and opportunities for training enhancement that are examined below.

The tables below identify the requisite suggested competency proficiency levels for each of the cyber actors, readily available training, and general comments.

Table 7. Survey of Currently Available Training for Competencies Relating to All Members of Police Service

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
All Members	1	1								

Course and Digital Competencies: All Members of Police Service

Digital Literacy and the Internet (1)

- Various short courses are widely available both online and in-person, including free unstructured awareness training through Microsoft at Digital Literacy | Microsoft.
- Basic Online Investigations (CPKN – Calgary Police Service)

Cyber Hygiene and Security (1)

- Cyber Security in the GC and Cybercrime Landscape (Canadian Centre for Cyber Security)
- Cyber Security of Internet of Things (IoT) (Canadian Centre for Cyber Security)

Additional Notes:

- There is insufficient availability of training and courses for rudimentary digital literacy and the internet and cyber hygiene and security. Online courses from virtual learning platforms such as Udemy, Coursera, and Edx offer basic courses on digital literacy.

- A lot of digital literacy and internet training at the basic level is catered to seniors.
- There are numerous reading materials and resources on the matter covering fundamental and basic concepts on a wide array of cyber-related topics. For example, Canadian Centre for Cyber Security https://cyber.gc.ca/en/guidance/cyber-security-home-and-office-secure-your-devices-computers-and-networks-itsap00007 and https://cyber.gc.ca/en/guidance/cyber-hygiene

Table 8. Survey of Currently Available Training for Competencies Relating to First Responders

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
First Responders*	1	2	2	1	1	1	1		2	1

Course and Digital Competencies – First Responders

Digital Literacy and the Internet (1)

- Various short courses are widely available both online and in-person, including free unstructured awareness training through Microsoft at Digital Literacy | Microsoft.
- Basic Online Investigations (CPKN – Calgary Police Service)

Cyber Hygiene and Security (2)

- Cyber Security in the GC and Cybercrime Landscape (Canadian Centre for Cyber Security)
- Cyber Security of Internet of Things (IoT) (Canadian Centre for Cyber Security)
- Cybercrime Investigations Level 1 (CPKN – Halifax Regional Police)
- Cyber Security in the GC for non-IT Employees (Canadian Centre for Cyber Security)

Cybercrime Awareness, Prevention and Victim Assistance

- Basic Online Investigations (CPKN – Calgary Police Service)

Open Source (1)

- Cybercrime Investigations Level 1 (CPKN - Halifax Regional Police) *Level 1/2

Cyber Legalities (1)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Improving Reporting of Cybercrime through Uniform Crime Reporting Survey (Statistic Canada)
- No specific training for cyber legalities at competency Level 1 although general police training (recruit training) generally identifies the concepts.

Data and Intelligence Analytics (1)

- Although no specific training was identified, all police services provide training for members of their service on various records management systems.

Cryptocurrency and Blockchain (1)

- Although various online platforms and in-person educational institutions offer courses in cryptocurrency awareness, none are geared toward law enforcement.

Digital Forensics (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Digital Forensics Essentials (SANS)
- Forensic Digital Imaging: Documenting and Presenting Visual (Justice Institute of British Columbia)
- Various digital forensic software vendors like Cellebrite and Magnet Forensics provide training on the use of their products that are used by first responders.

Network Forensics (1)

- No specific training identified for competency Level 1. Training starts at competency Level 2 and higher through providers like SANs and CompTIA.

Additional Notes:

- There is insufficient availability of training and courses for basic digital literacy and the internet, cyber hygiene and security, cryptocurrency and blockchain, and network forensics.
- Online platforms like Udemy, Coursera, and Edx have numerous online courses that provide introductory or Level 1 information on these topics.
- A lot of Digital Literacy and internet training at this basic level is catered to seniors.
- Less training available for lower-level digital competencies; instead, more offer resources such as PDFS and YouTube videos sharing foundational information.

Table 9. Survey of Current Widely Available Training for Competencies Relating to General Duties Investigators or Detectives

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
General Detectives*	2	2	2	2	2	2	2		2	2

Course and Digital Competencies General Duties Investigator/Detective

Digital Literacy and the Internet (2)

- Various short courses are widely available both online and in-person. The most common training is provided through completion of the CompTIA IT Fundamentals (ITF +).

Cyber Security and Hygiene (2)

- Cyber Security in the GC and Cybercrime Landscape (Canadian Centre for Cyber Security)
- Cyber Security of Internet of Things (IoT) (Canadian Centre for Cyber Security)
- Cybercrime Investigations Level 1 (CPKN – Halifax Regional Police)
- Cyber Security in the Government of Canada for non-IT Employees (Canadian Centre for Cyber Security)

Cybercrime, Prevention, and Victim Assistance (2)

- Basic Online Investigations (CPKN – Calgary Police Service)
- No specific training identified regarding victim assistance and prevention

Open Source (2)

- Using the Internet as an Intelligence Tool (INTINT) (Canadian Police College)
- Cybercrime Investigations Level 1 (CPKN – Halifax Regional Police)
- Internet Investigations – Level 2 (Holland College)
- Internet Investigations – LITE (Holland College)
- The Facebook Guide for Investigators (Holland College)

Cyber Legalities (2)

- Law of Data Security & Investigations (SANS) – Level 2/3
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (2)

- Introduction to Intelligence Analysis (Toddington) – Level 2/3
- Criminal Intelligence (Analysis 202Eca) (Toddington) – Level 2/3
- Strategic Intelligence (Analysis 203E SA) (Toddington) – Level 2/3

Cryptocurrency and Blockchain (2)

- Although online platforms and in-person educational institutions offer courses in Cryptocurrency awareness and understanding none are geared to law enforcement.

Digital Forensics (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Digital Forensics Essentials (SANS)
- Forensic Digital Imaging: Documenting and Presenting Visual (Justice Institute of British Columbia)
- Various digital forensic software vendors like Cellebrite and Magnet Forensics provide training on the use of their products that are used by first responders.

Network (Cloud) Forensics (2)

- Basic Network & Database Security (IBM by Edx)
- Introduction to Networks and Hardware (International Association of Chiefs of Police)
- CompTIA Network + * Levels 2/3

Additional Notes:

- Data and Intelligence Analytics through Toddington contain two parts bridging it to a Level 2/3
- Cybercrime, Prevention, and Victim Assistance, Cryptocurrency and Blockchain, and Network Forensics training at these levels are insufficient.

Table 10. Currently Available Training for Competencies Relating to Cyber-related Intermediate Technicians

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
Intermediate Investigators *	3	3	3	2	2	2	2	3	3	3

Courses and Digital Competencies Cyber-related Intermediate Technicians

Digital Literacy and the Internet (3)

- CompTIA A+ (CompTIA)

Cyber Hygiene and Security (3)

- Cyber Security in the GC Boot Camp (Canadian Centre for Cyber Security) *boot camp progresses quickly from basic to advanced concepts (Level 2/3)
- Foundations – Computers, Technology & Security (SANS) *Level 2/3 – offers computer concepts, networking fundamentals, cyber security concepts, introduction to forensics.
- Introduction to Cyber Security (SANS)* Levels 2/3
- CompTIA Security + (CompTIA)

Cybercrime, Prevention, and Victim Assistance (3)

- No specific training identified

Open Source (2)

- Using the Internet as an Intelligence Tool (INTINT) (Canadian Police College)
- Cybercrime Investigations Level 1 (CPKN – Halifax Regional Police)
- Internet Investigations – Level 2 (Holland College)
- Internet Investigations – LITE (Holland College)
- The Facebook Guide for Investigators (Holland College)

Cyber Legalities (2)

- Law of Data Security & Investigations (SANS) – Level 2/3
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (2)

- Introduction to Intelligence Analysis (Toddington) *Level 2/3
- Criminal Intelligence (Analysis 202Eca) (Toddington) *Level 2/3
- Strategic Intelligence (Analysis 203E SA) (Toddington) *Level 2/3

Programming and Scripting (3)

- ICS/SCADA Security Essentials (SANS)
- Blue Team Fundamentals: Security Operations and Analysis (SANS)
- Education and training in programming and scripting is widely available through private and public cyber education providers.

Cryptocurrency and Blockchain (2)

- Although online platforms and in-person educational institutions offer courses in cryptocurrency awareness and understanding, none are geared to law enforcement.

Digital Forensics (3)

- Digital Forensics Essentials (SANS)
- Mobile Device Acquisition & Analysis (Canadian Police College)

Network (Cloud) Forensics (3)

- Internet Evidence Analysis (Canadian Police College)
- Network Investigative Techniques Course (Canadian Police College)
- Mobile Device Acquisition and Analysis (Canadian Police College)
- Cloud Security Essentials (SANS)
- Live Analysis Workshop (Canadian Police College) – Level 3

Additional Notes:

- There is insufficient availability of training and courses in cryptocurrency and blockchain.
- Data and Intelligence Analytics through Toddington contain two parts bridging it to a Level 2/3
- Numerous college-level courses offer programming and scripting courses that would meet competency requirement. For example, course offered at McMaster University: Python for Advanced collection.

Table 11. Currently Available Training for Competencies Relating to Outreach, Prevention and Victim Assistance

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
Outreach Prevention/ Victim Assistance *	2	2	4	2	2	1	2		2	2

Courses and Digital Competencies Outreach Victim Liaison Professionals

Digital Literacy and the Internet (2)

- Various short courses are widely available both online and in-person. The most common training is provided through completion of the CompTIA IT Fundamentals (ITF +).

Cyber Hygiene and Security (2)

- Cyber Security in the GC and Cybercrime Landscape (Canadian Centre for Cyber Security)
- Cyber Security of Internet of Things (IoT) (Canadian Centre for Cyber Security)
- Cybercrime Investigations Level 1 (CPKN – Halifax Regional Police)
- Cyber Security in the GC for non-IT Employees (Canadian Centre for Cyber Security)

Cybercrime, Prevention and Victim Assistance (4)

- Leading Cybersecurity Change: Building a Security-Based Culture (SANS)
- No specific training identified for victim assistance issues related to cybercrime.

Open Source (2)

- Using the Internet as an Intelligence Tool (INTINT) (Canadian Police College)
- Cybercrime Investigations Level 1 (CPKN – Halifax Regional Police)
- Internet Investigations – Level 2 (Holland College)
- Internet Investigations – LITE (Holland College)
- The Facebook Guide for Investigators (Holland College)

Cyber Legalities (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Law of Data Security & Investigations (SANS) – Level 2/3
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (1)

- Although no specific training was identified, all police services provide training for members of their service on various records management systems.

Cryptocurrency and Blockchain (2)

- Although online platforms and in-person educational institutions offer courses in cryptocurrency awareness and understanding, none are geared to law enforcement.

Digital Forensics (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Digital Forensics Essentials (SANS)
- Forensic Digital Imaging: Documenting and Presenting Visual (Justice Institute of British Columbia)
- Various digital forensic software vendors like Cellebrite and Magnet Forensics provide training on the use of their products that are used by first responders.

Network (Cloud) Forensics (2)

- Basic Network & Database Security (IBM by Edx)
- Introduction to Networks and Hardware (International Association of Chiefs of Police)

Additional Notes:

- There is insufficient availability of training and courses for digital literacy and the internet, cybercrime prevention and victim assistance, data and intelligence analytics, and cryptocurrency and blockchain.
- Numerous college-level courses offer programming and scripting courses that would meet competency requirement. For example, course offered at McMaster University: Python for Basic Collection and Python for Advanced collection.

Table 12. Currently Available Training for Competencies Relating to Online Internet-based Investigator

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
Open-Source Investigator*	4	3	2	4	3	3	3	3	2	3

Courses and Digital Competencies Online Internet-Based Investigator (ONSIT)

Digital Literacy and the Internet (4)

- Various Comp TIA courses including A+, Network+ and Security+

Cyber Hygiene and Security (3)

- Cyber Security in the GC Boot Camp (Canadian Centre for Cyber Security) *boot camp progresses quickly from basic to advanced concepts (Level 2/3)
- Foundations – Computers, Technology & Security (SANS) *Level 2/3 – offers computer concepts, networking fundamentals, cyber security concepts, introduction to forensics.
- Introduction to Cyber Security (SANS)* Levels 2/3
- CompTIA Security + (CompTIA)

Cybercrime, Prevention and Victim Assistance (1)

- Basic Online Investigations (CPKN – Calgary Police Service)
- No specific training identified regarding victim assistance and prevention

Open Source (4)

- Advanced Open-Source intelligence (AOSINT) (Canadian Police College)
- Practical Open-Source Intelligence (OSINT) Analysis Automation (SANS)
- Certified Social Media Intelligence Expert (McAfee Institute)
- Certified Social Media Intelligence Analyst (McAfee Institute)

Cyber Legalities (3)

- Law of Data Security & Investigations (SANS) – Level 2/3
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (3)

- Introduction to Intelligence Analysis (Toddington) * Level 2/3
- Criminal Intelligence (Analysis 202Eca) (Toddington) *Level 2/3
- Strategic Intelligence (Analysis 203E SA) (Toddington) *Level 2/3
- Cyber Threat Intelligence (SANS) * Level 3-4

Cryptocurrencies and Blockchain (3)

- Blockchain and Smart Contract Security (SANS) – Level 3
- Although online platforms and in-person educational institutions offer courses in the use of Cryptocurrency none are geared to law enforcement.

Digital Forensics (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – level 1-2
- Digital Forensics Essentials (SANS)
- Forensic Digital Imaging: Documenting and Presenting Visual (Justice Institute of British Columbia)
- Various digital forensic software vendors like Cellebrite and Magnet Forensics provide training on the use of their products that are used by first responders.

Network Forensics (3)

- Internet Evidence Analysis (Canadian Police College)
- Network Investigative Techniques Course (Canadian Police College)
- Mobile Device Acquisition and Analysis (Canadian Police College)
- Cloud Security Essentials (SANS)
- Live analysis Workshop (Canadian Police College)
- ICS Cybersecurity In-Depth (SANS) *level 3

Additional Notes:

- Training widely available that complements competency profiles.

Table 13. Currently Available Training for Competencies Relating to Cybercrime Analysts

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
Cybercrime Analyst*	3	3	2	3	2	4	4	4	2	3

Courses and Digital Competencies Cybercrime Analysts

Digital Literacy and the Internet (3)

- CompTIA A+ (CompTIA)

Cyber Hygiene and Security (3)

- Cyber Security in the GC Boot Camp (Canadian Centre for Cyber Security) *boot camp progresses quickly from basic to advanced concepts (Level 2-3)
- Foundations – Computers, Technology & Security (SANS) *Level 2/3 – offers computer concepts, networking fundamentals, cyber security concepts, introduction to forensics.
- Introduction to Cyber Security (SANS)
- CompTIA Security + (CompTIA)

Cybercrime, Prevention, and Victim Assistance (2)

- Basic Online Investigations (CPKN – Calgary Police Service)
- No specific training identified regarding victim assistance and prevention

Open Source (3)

- Using the Internet as an Investigative Research Tool (Toddington)
- Social Media Intelligence & Investigation (Toddington)
- Open-Source Intelligence (OSINT) Gathering and Analysis (SEC487) – SANS

Cyber Legalities (2)

- Law of Data Security & Investigations (SANS) – Level 2/3
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (4)

- Cyber Threat Intelligence (SANS)

Cryptocurrency and Blockchain (3/4)

- Blockchain and Smart Contract Security (SANS) – Level 3
- Although online platforms and in-person educational institutions offer courses in the use of Cryptocurrency none are geared to law enforcement.

Programming and Scripting (2/3)

- Basic Network & Data Base Security (IBM with Edx)
- Blue Team Fundamentals: Security Operations and Analysis (SANS)
- ICS/SCADA Security Fundamentals (SANS)
- Education and training in programming and scripting is widely available through private and public cyber education providers.

Digital Forensics (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Digital Forensics Essentials (SANS)
- Forensic Digital Imaging: Documenting and Presenting Visual (Justice Institute of British Columbia)
- Various digital forensic software vendors like Cellebrite and Magnet Forensics provide training on the use of their products that are used by first responders.

Network Forensics (3)

- Internet Evidence Analysis (Canadian Police College)
- Network Investigative Techniques Course (Canadian Police College)
- Mobile Device Acquisition and Analysis (Canadian Police College)
- Cloud Security Essentials (SANS)
- Live analysis Workshop (Canadian Police College)
- ICS Cybersecurity In-Depth (SANS) *Level 3

Additional Notes:

- Training widely available that complements competency profiles.

Table 14. Currently Available Training for Competencies Relating to Digital Forensic Examiner

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
Digital Forensic Examiner*	4	4	2	3	3	3	4	3	5	5

Courses and Digital Competencies Digital Forensic Examiner

Digital Literacy and the Internet (4)

- Various Comp TIA courses including A+, Network+ and Security+

Cyber Hygiene and Security (4)

- Network Penetration Testing and Ethical Hacking (SANS)

Cybercrime, Prevention, and Victim Assistance (2)

- Basic Online Investigations (CPKN – Calgary Police Service)
- No specific training identified regarding victim assistance and prevention

Open Source (3)

- Using the Internet as an Investigative Research Tool (Toddington)
- Social Media Intelligence & Investigation (Toddington)
- Open-Source Intelligence (OSINT) Gathering and Analysis (SEC487) - SANS

Cyber Legalities (3)

- Law of Data Security & Investigations (SANS) – Level 2/3* US Law, no equivalent Canadian law course
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (3)

- Introduction to Intelligence Analysis (Toddington) – Level 2/3
- Criminal Intelligence (Analysis 202Eca) (Toddington) – Level 2/3
- Strategic Intelligence (Analysis 203E SA) (Toddington) – Level 2/3
- Cyber Threat Intelligence (SANS) – Level 3/4

Cryptocurrency and Blockchain (3/4)

- Blockchain and Smart Contract Security (SANS) – Level 3
- Although online platforms and in-person educational institutions offer courses in the use of cryptocurrency, none are geared to law enforcement.

Programming and Scripting (3)

- Basic Network & Data Base Security (IBM with Edx)
- Blue Team Fundamentals: Security Operations and Analysis (SANS)
- ICS/SCADA Security Fundamentals (SANS)
- Education and training in programming and scripting is widely available through private and public cyber education providers.

Digital Forensics (4/5)

- Computer Forensics Examiners (Canadian Police College)
- Battlefield & Data Acquisition (SANS)
- Computer Forensic Examiner (CMPFOR) (Canadian Police College)
- Smartphone Forensic Analysis In-Depth (SANS)
- Advanced JTAG Mobile Forensics Training (Justice Institute of British Columbia)
- Cellebrite JTAG Extraction and Decoding (Justice Institute of British Columbia)
- TEEL Cellebrite 5 day Mobile Device Examination (Justice Institute of British Columbia)

Network (Cloud) Forensics (4/5)

- Advanced Network Forensics and Incident Response (SANS)
- Advanced Security Essentials – Enterprise Defender (SANS)
- Cloud Security Monitoring and Threat Detection (SANS)
- Network Penetration Testing and Ethical Hacking (SANS)
- Advanced Exploit Development for Penetration (SANS)

Additional Notes:

- Sufficient trainings and courses in higher level digital competencies in both digital forensics and Network forensics. **Only a small sample of available offerings are listed above**.

Table 15. Currently Available Training for Competencies Relating to Cybercrime Investigator

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
Cybercrime Investigator*	4	3	3	3	4	3	4	2	2	2

Courses and Digital Competencies Cybercrime Investigator

Digital Literacy and the Internet (4)

- Various Comp TIA courses including A+, Network+ and Security+

Cyber Hygiene and Security. (3)

- Cyber Security in the GC Boot Camp (Canadian Centre for Cyber Security) *boot camp progresses quickly from basic to advanced concepts (Level 2/3)
- Foundations – Computers, Technology & Security (SANS) *Level 2/3 – offers computer concepts, networking fundamentals, cyber security concepts, introduction to forensics.
- Introduction to Cyber Security (SANS)* Levels 2/3
- CompTIA Security + CompTIA

Cybercrime, Prevention, and Victim Assistance. (3)

- Certified Expert in Cyber Investigations (McAfee Institute) *note: does touch on some topics that may not be as relevant i.e., retail crime.
- No training identified that deals specifically with victim assistance for cybercrime.

Open Source (3)

- Using the Internet as an Investigative Research Tool (Toddington)
- Social Media Intelligence & Investigation (Toddington)
- Open-Source Intelligence (OSINT) Gathering and Analysis (SEC487) – SANS

Cyber Legalities (4)

- Law of Data Security & Investigations (SANS) – Level 2/3 *US Law, no equivalent Canadian law course
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (3)

- Introduction to Intelligence Analysis (Toddington) * Level 2/3
- Criminal Intelligence (Analysis 202Eca) (Toddington) *Level 2/3
- Strategic Intelligence (Analysis 203E SA) (Toddington) *Level 2/3
- Cyber Threat Intelligence (SANS) * Level 3/4

Cryptocurrency and Blockchain (3/4)

- Blockchain and Smart Contract Security (SANS) *Level 3
- Although online platforms and in-person educational institutions offer courses in the use of cryptocurrency, none are geared to law enforcement.

Programming and Scripting (2)

- Basic Network & Database Security (IBM with edx)
- Education and training in programming and scripting is widely available through private and public cyber education providers.

Digital Forensics (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Digital Forensics Essentials (SANS)
- Forensic Digital Imaging: Documenting and Presenting Visual (Justice Institute of British Columbia)
- Various digital forensic software vendors like Cellebrite and Magnet Forensics provide training on the use of their products that are used by first responders.

Network (Cloud) Forensics (2)

- Basic Network & Database Security (IBM by Edx)
- Introduction to Networks and Hardware (International Association of Chiefs of Police)
- CompTIA Network + *Level 2/3

Additional Notes:

- Training widely available that complements competency profiles.

Table 16. Currently Available Training for Competencies Relating to Managers and Leaders

	Digital Literacy and the Internet	Cyber Hygiene – Cyber Security	Cybercrime Awareness, Prevention and Victim Assistance	Open-Source Intelligence and Evidence Collection	Cyber Legalities	Cyber Data and Intelligence Analytics	Crypto-currency and Blockchain	Programming and Scripting	Digital Forensics	Network (Cloud) Forensics
Leadership*	3	3	3	2	4	2	2		2	2

Course and Digital Competencies Managers and Leaders

Digital Literacy and the Internet (3)

- CompTIA A+ (CompTIA)

Cyber Hygiene and Security (3)

- Cyber Security in the GC Boot Camp (Canadian Centre for Cyber Security) *boot camp progresses quickly from basic to advanced concepts (Level 2/3)
- Foundations – Computers, Technology & Security (SANS) *Level 2/3 – offers computer concepts, networking fundamentals, cyber security concepts, introduction to forensics.
- Introduction to Cyber Security (SANS)* Levels 2/3
- CompTIA Security + CompTIA

Cybercrime, Prevention, and Victim Assistance (4)

- Leading Cybersecurity Change: Building a Security-Based Culture (SANS)
- No training identified that deals specifically with victim assistance for cybercrime.

Open Source (2)

- Using the Internet as an Intelligence Tool (INTINT) (Canadian Police College)
- Cybercrime Investigations Level 1 (CPKN – Halifax Regional Police)
- Internet Investigations – Level 2 (Holland College)
- Internet Investigations – LITE (Holland College)
- The Facebook Guide for Investigators (Holland College)

Cyber Legalities (3/4)

- Law of Data Security & Investigations (SANS) – level 2/3 *US Law, no equivalent Canadian law course
- Internet Investigations – Level 1 – 2021 SYR APA-III-0812 (Atlantic Police College)
- Digital Technologies for Investigators (Canadian Police College) – Level 2/3
- Cybercrime Investigators Course (Canadian Police College)

Data and Intelligence Analytics (2)

- Introduction to Intelligence Analysis (Toddington) *Level 2/3
- Criminal Intelligence (Analysis 202Eca) (Toddington) *Level 2/3
- Strategic Intelligence (Analysis 203E SA) (Toddington) *Level 2/3

Cryptocurrency and Blockchain (2)

- Although online platforms and in-person educational institutions offer courses in cryptocurrency awareness and understanding, none are geared to law enforcement.

Digital Forensics (2)

- Digital Evidence: Frontline Investigations (CPKN – York Regional Police) – Level 1/2
- Digital Forensics Essentials (SANS)
- Forensic Digital Imaging: Documenting and Presenting Visual (Justice Institute of British Columbia)
- Various digital forensic software vendors like Cellebrite and Magnet Forensics provide training on the use of their products that are used by first responders.

Network (Cloud) Forensics (2)

- Basic Network & Database Security (IBM by Edx)
- Introduction to Networks and Hardware (International Association of Chiefs of Police)
- CompTIA Network + * Level 2/3

Additional Notes:

- Insufficient training in Digital Literacy and the Internet, Cybercrime Prevention and Victim Assistance, Cryptocurrency and Blockchain and Network Forensics at the prescribed level.

5.2. Training Gap Analysis

Notwithstanding the limitations of the training survey, a review of readily available training identified the following themes for each of the digital competencies:

Digital Literacy and the Internet

- There is a wide range of training available, especially from online platforms.
- A lot of online training in the digital literacy area is unstructured.
- Digital literacy training does not require a law enforcement lens at lower competency levels.
- Training is lacking at the most basic levels.

Cyber Hygiene and Security

- Self-directed online resources are offered at a basic level.
- Available cyber hygiene training with a law enforcement lens is lacking, especially at lower competency levels.
- Formal training appears to be limited to the higher levels of cyber security.
- Training is expensive.
- Private sector and publicly funded educational institutions offer training certification in cyber security.

Cyber Legalities

- Little training offered at all levels – specifically looking at Canadian law.
- Expert witness training is offered only by Canadian Police College - Technical Crime Learning Institute.

Victim Assistance

- Little training offered at all levels.
- Some of the fundamental investigative and interviewing courses address how to talk to victims and witnesses. None, however, are specifically geared to victims of cybercrime.
- None of the courses offered by Canadian police learning institutions include curriculum on victim assistance.

Digital Forensics

- Training and courses are lacking at the more basic levels.
- Extensive training offered at higher competency levels by police training institutions and private sector training providers.

Data and Intelligence Analytics

- Training and courses lacking at the more basic levels.
- Advanced training offered by police training institutions and private sector training providers.
- Colleges and universities offer wide range of courses and programs in data analysis.

Cryptocurrency and Blockchain

- Training for use and awareness of cryptocurrency and blockchain in a law enforcement context is lacking at all levels.
- Numerous colleges and universities, including online learning platforms (Udemy, Coursera, etc.), offer courses in the theory and use of cryptocurrency and blockchain at introductory to advanced levels.

Programming and Scripting

- Courses on programming and scripting at all levels are widely available through universities, colleges, and private sector providers.

Digital Forensics

- Few training opportunities at lower competency levels
- Wide range of training offered by police training institutions, public education institutions, and private sector providers.

Network Forensics

- Few training opportunities at lower competency levels
- Wide range of training offered by police training institutions, public education institutions, and private sector providers.

It appears that there are numerous training opportunities for those roles considered as specialist. Specifically, Cyber-related Intermediate Technicians, Digital Forensic Examiners, Cybercrime Investigators, Cybercrime Analysts and Online Internet-based Investigators. The Canadian Police College (CPC), for example, through the Technical Crime Learning Institute (TCLI), provides highly specialized training in digital forensic examination, cybercrime investigation, and open-source intelligence gathering. These courses fulfill most of the training requirements of the specialist roles noted above. The TCLI courses form the primary training requirements of the RCMP Computer Forensic Examiner understudy program.

Table 17. Specialized Courses Offered through Canadian Police College Technical Crime Learning Institute

Forensics	Cybercrime – Cyber-enabled Crime
• Computer Forensic Examiner • Internet Evidence Analysis • Network Investigative Techniques • Mobile Device Acquisition and Analysis • Live Analysis Workshop • Registry Analysis Workshop • Technical Court Expert and Testimony	• Digital Technologies for Investigators • Cybercrime Investigators Course • Using the Internet as an Intelligence Tool • Advanced Open-Source Intelligence Course • Canadian Internet Child Exploitation • Advanced Internet Child Exploitation • Peer-to-Peer Investigator Course

Source: (Canadian Police College, 2021)

The specialized courses offered through CPC-TCLI are complemented by numerous private sector providers such as the SANS Institute, which also offers numerous specialized technical courses.

Competency attainment in the specialized cyber roles goes beyond attending courses. Highly specialized roles such as Digital Forensic Examiners also require mentorship (Baron & Le Khac, 2021, p. 15). Less specialized roles, however, can conceivably achieve Level 1 or 2 competency proficiency through education alone. Nevertheless, it is in these areas that training opportunities are lacking or incomplete.

Consider the roles of First Responder and General Duties Investigator/Detective: the ubiquity of digital evidence, coupled with the changing nature of crime, means that in terms of sheer volume front line officers arguably have the greatest exposure to incidents that lie on the cyber spectrum. While individual police services partnered with CPKN have built cyber training aimed at first responders, there are no training options that are widely and readily available for first responders or general duties detectives that fulfill the totality of the identified competency through a single course or modular course offering.

As it stands, Canadian law enforcement agencies must send their first responder and general duties detective members on several courses to meet the recommended competency levels—a feat which is undoubtedly beyond any service's physical and financial capacity.

6. Recommendations

The following recommendations are based on the research regarding global practice, focus groups consultations, the survey of training opportunities, and the training gap analysis:

1. **Build training capacity for non-specialized cyber roles.**

   Cyber-related training for non-specialized cyber roles requires investment to enhance training capacity and competency attainment. The ubiquity of digital evidence and the changing nature of crime requires a unified approach by Canadian law enforcement to build front line capacity to deal with cyber-related issues.

   Primarily led by the CPC-TCLI and private sector providers such as the SANS Institute, training for specialized roles at competency Levels 3 and 4 is already well established.

2. **Build readily and easily accessible cyber hygiene training with a curriculum based on the All Members of the Police Service competency profile.**

   Focusing on basic cyber hygiene, this short course should be designed for high-volume and accessible delivery.

3. **Rebuild CPKN's Cybercrime Investigations training with a curriculum based on the First Responder competency profile.**

   The competency profile for First Responders introduces elements such as victim assistance and cryptocurrency awareness that not included in the current version Cybercrime Investigations Level 1. The rebuilt version could be delivered as a single course or through several modules that focus on one or more competencies. The module program could include the Digital Evidence: Frontline Investigations course as a module. Completion of requisite modules would result in completion of First Responders or General Duties Investigators/Detectives competency requirements. This course should be designed for high-volume easily accessible delivery.

4. **Build readily and easily accessible cyber training with a curriculum based on the General Duties Investigators/Detectives competency profile.**

   High-volume cyber and cyber-enabled crimes such as identity theft and online frauds are generally investigated by local-level detectives in detachments or divisions. The competency profile of General Duties Investigators/Detectives requires competencies beyond those recommended for first responders. This course should build on the concepts and curriculum of the rebuilt Cybercrime Investigations Level 1 course.

5. **Work with partners to build victim assistance modules with competency Levels 1- and 2-based curricula.**

   There is very little training on cybercrime victim assistance. These modules will complement both specialized and non-specialized roles and introduce a victim-centred approach to cyber investigations.

6. **Work with partners to build or identify training in Cryptocurrency and Blockchain for law enforcement with competency Levels 1, 2, and 3 curricula.**

   There is very little training available in this area that has an operational law enforcement lens. This training maybe well suited to a modular approach for each competency level.

7. **Continue to liaise with CACP E-Crimes Committee and National Police Service Cybercrimes Committee for annual review, evaluation, and validation of digital competency dictionary and profiles.**

   Although the competency dictionary and the competency profiles were designed to be evergreen, continued evaluation of a competency's validity and completeness is an essential component in any competency-based management framework. As the primary governance bodies for cybercrime in Canada, the CACP E-Crimes Committee and the National Police Services Cybercrime Committee are well suited to provide annual evaluation and validation of the digital competency profiles.

8. **Continue evaluation of courses and cyber training to ensure they contain valid competency-based curricula.**

   A corollary of Recommendation 7 is that changes to the competency dictionary may require changes to the training or course curriculum.

9. **Consider partnerships with public education institutions or private sector providers.**

   Many public educational institutions and private sector training providers are active in the cyber training space. Courses and training may already exist or require minor tweaks to fit the law enforcement context. Partnerships with existing cyber training providers may also provide access to a wealth of subject matter experts.

7. Works Cited

Armstrong, P. (2021, 06 04). *Center for Teaching - Bloom's Taxonomy*. Retrieved from Vanderbuilt University: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

Association of Police and Crime Commissioners. (2020). *National Policing Digital Strategy. Digital, Data and Technology Strategy 2020 - 2030.* London: Association of Police and Crime Commissioners. Retrieved 06 05, 2021, from https://www.apccs.police.uk/media/4886/national-policing-digital-strategy-2020-2030.pdf

Baron, A., & Le Khac, N. A. (2021, 08 08). *Cybercrime Competencies – A Training and Education Perspective.* University College Dublin, School of Computer Science and Infomatics. Dublin: University College Dublin.

Canadian Police College. (2021, 04 22). *Technical Crime Learning Institute*. Retrieved 06 02, 2021, from Canadain Police College: https://www.cpc-ccp.gc.ca/programs-programmes/technological-technologique/index-eng.htm#a1

Canadian Police Knowledge Network. (2020, 03 23). *Competencies Dictionary*. Retrieved 05 25, 2021, from Canadian Police Knowledge Network - Community of Practice: https://lms.cpkn.ca/goto.php?target=wiki_417

Canadian Police Knowledge Network. (2020). *White Paper Competency-Based Policing in Canada: An Integal Component for Transparency and Accountable Policing.* Charlettown, Prince Edward Island: Canadian Police Knowledge Network.

Carnegie Mellon University. (2018). *Cyber Investigator Certificate Program*. Retrieved from FBI - CICP: https://fbi-cicp.cert.org/lms

Council of Europe. (2001, November 23). Convention on Cybercrime. *European Treaty Series - No. 185.* Budapest: Council of Europe.

European Commission. (2019, 06 06). *Press Release: Security Union: Commission receives mandate to start negotiating international rules for obtaining electronic evidence.* Retrieved from European COmmission - Press Corner: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2891

European Cybercrime Training and Education Group. (2020, August 27). *Cybercrime Training Competencies Framework Introduction.* Retrieved from Cybercrime Training Competency Framework: https://www.ecteg.eu/tcf/co/TCG_OpaleModule_4.html

European Cybercrime Training and Education Group. (2021, February 08). *E-FIRST: First Responders E-Learning Package*. Retrieved from European Cybercrime Training and Education Group: https://www.ecteg.eu/running/first-responders/

Europol. (2018). *Internet organized Crime Threat Assessment (IOCTA) 2018.* The Hauge : European Union Agency for Law Enforcemet Cooperations.

Federal Bureau of Investigation. (2016, October 19). *National Cyber Security Awareness Month.* Retrieved from Federal Bureau of Investigation: https://www.fbi.gov/news/stories/online-cyber-training-for-law-enforcement-first-responders

Government of Canada. (2020, 12 02). *Skills and Competencies Taxonomy*. Retrieved 06 04, 2021, from Government of Canada: https://noc.esdc.gc.ca/SkillsTaxonomy/SkillsTaxonomyWelcome

Greenwood, K. (2020, December). Policing, Competencies, and Building a New Normal. *Canadian Police Chief Magazine*, pp. 12-13.

Her Majesty's Inspectorate of Constabulary. (2015). *Real lives, real crimes: A study of digital crime and policing.* London: Her Majesty's Inspectorate of Constabulary. Retrieved from https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

Kowalski, M. (2002). *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.* Ottawa: Statistics Canada, Canadian Centre for Justice Statistics.

Lincolnshire Constabulary. (2021, February 02). *Lincolnshire Police Cyber Crime Strategy.* Retrieved from Lincolnshire Police: https://www.lincs.police.uk/media/252353/cyber-crime-strategy.pdf

Manhattan District Attorney's Office. (2021, February 01). *Our Work: Cybercrime*. Retrieved from Manhattan District Attoney's Office: https://www.manhattanda.org/our-work/cybercrime/

Mazowita, B., & Vezina, M. (2014, September 25). Police-reported cybercime in Canada, 2012. *Juristat*.

NW3C. (2021, February 9). *NW3C Certifications*. Retrieved from NW3C: https://www.nw3c.org/certifications/AssessmentResults#certificationassessment

Ontario Provincial Police (1). (2016). *From Frontline to Online OPP Cyber Stategy.* Unpublished.

Ontario Provincial Police (2). (2016). *Ontario Provincial Police Cybercrime Strategy: From Frontline to Online.* Orillia, ON: Ontario Provincial Police.

Robertson, J. G. (2019). *The Impact of Digital Society on Police Recuit Training in Canada.* Ontario Tech University, Faculty of Education. Oshawa: Ontairio Technical University.

Royal Canadian Mounted Police. (2015). *Royal Canadian Mounted Police Cybercrime Strategy.* Ottawa: Her Majesty the Queen in Right of Canada as represented by the Royal Canadian Mounted Police.

Royal Canadian Mounted Police. (2021, January 27). *Cybercrime:an overview of incidents and issues in Canada*. Retrieved from Royal Canadian Mounted Police: https://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec2

Siden, D. (2017, July 4). Meaningful Evidence. Non-Specialists trained to triage digital devices. *Gazette Magazine Vol 79 No 3.*, p. 16.

Sobusial-Fischanaller, M., & Vandermeer, Y. (2016). *Cybercrime Training Governance Model: Cybercrime Training Competency Framework.* Retrieved from Council of Europe: https://rm.coe.int/3148-2-3-ecteg-16-cy-train-module/1680727f34

Statistics Canada. (2019, November 08). *Canadian Internet Use Survey*. Retrieved from Statistics Canada: https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm

Statistics Canada. (2021, January 25). *Police-reported cybercrime, by cyber-related violation, Canada (selected police services)*. Retrieved from Statistics Canada: https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000101

Statistics Canada. (2021, February 04). *Table 22-10-0083-01 Internet use by province*. Retrieved from Statistics Canada: https://doi.org/10.25318/2210008301-eng

Statistics Canada. (2021, February 02). *Telecommunications: Connecting Canadains*. Retrieved from Statistics Canada: https://www.statcan.gc.ca/eng/subjects-start/digital_economy_and_society/telecommunications

Thatcher, A. (2017, July 4). Cybercime on the front line. *Gazett Magazine*, p. 17.

The Council of Europe. (2020). *Budapest Convention and related standards*. Retrieved from Council of Europe: https://www.coe.int/en/web/cybercrime/the-budapest-convention

The Expert Panel on the Future of Canadian Policing Models. (2014). *Policing Canada in the 21st Century: New Polcing for New Challenges.* Ottawa: The Council of Canadian Academies.

University of Waterloo. (2021, 06 04). *Bloom's Taxonomy. Centre for Teaching Excellence*. Retrieved from University of Waterloo.

CANADIAN POLICE KNOWLEDGE NETWORK
RÉSEAU CANADIEN DU SAVOIR POLICIER

www.cpkn.ca