RCMP
ROYAL CANADIAN MOUNTED POLICE

Cybercrime:
AN OVERVIEW OF INCIDENTS AND ISSUES IN CANADA

Royal Canadian Mounted Police
Gendarmerie royale du Canada

Canada

CAT. NO.: PS64-116/2014E-PDF
ISBN: 978-1-100-24379-5

Executive Summary

Cybercrime: an overview of incidents and issues in Canada is the RCMP's first report on cybercrime, and focuses on aspects of the cybercrime environment that affect Canada's public organizations, businesses and citizens in real and harmful ways.

This report covers a broad range of criminal offences where the Internet and information technologies are used to carry out illegal activities. It describes select crimes in Canada's digital landscape to show the rising technical complexity, sophistication and expansion of cybercrime. While difficult to measure, these crimes show no sign of slowing in Canada.

The RCMP breaks cybercrime into two categories:

- ***technology-as-target*** - criminal offences targeting computers and other information technologies, such as those involving the unauthorized use of computers or mischief in relation to data, and;

- ***technology-as-instrument*** - criminal offences where the Internet and information technologies are instrumental in the commission of a crime, such as those involving fraud, identity theft, intellectual property infringements, money laundering, drug trafficking, human trafficking, organized crime activities, child sexual exploitation or cyber bullying.

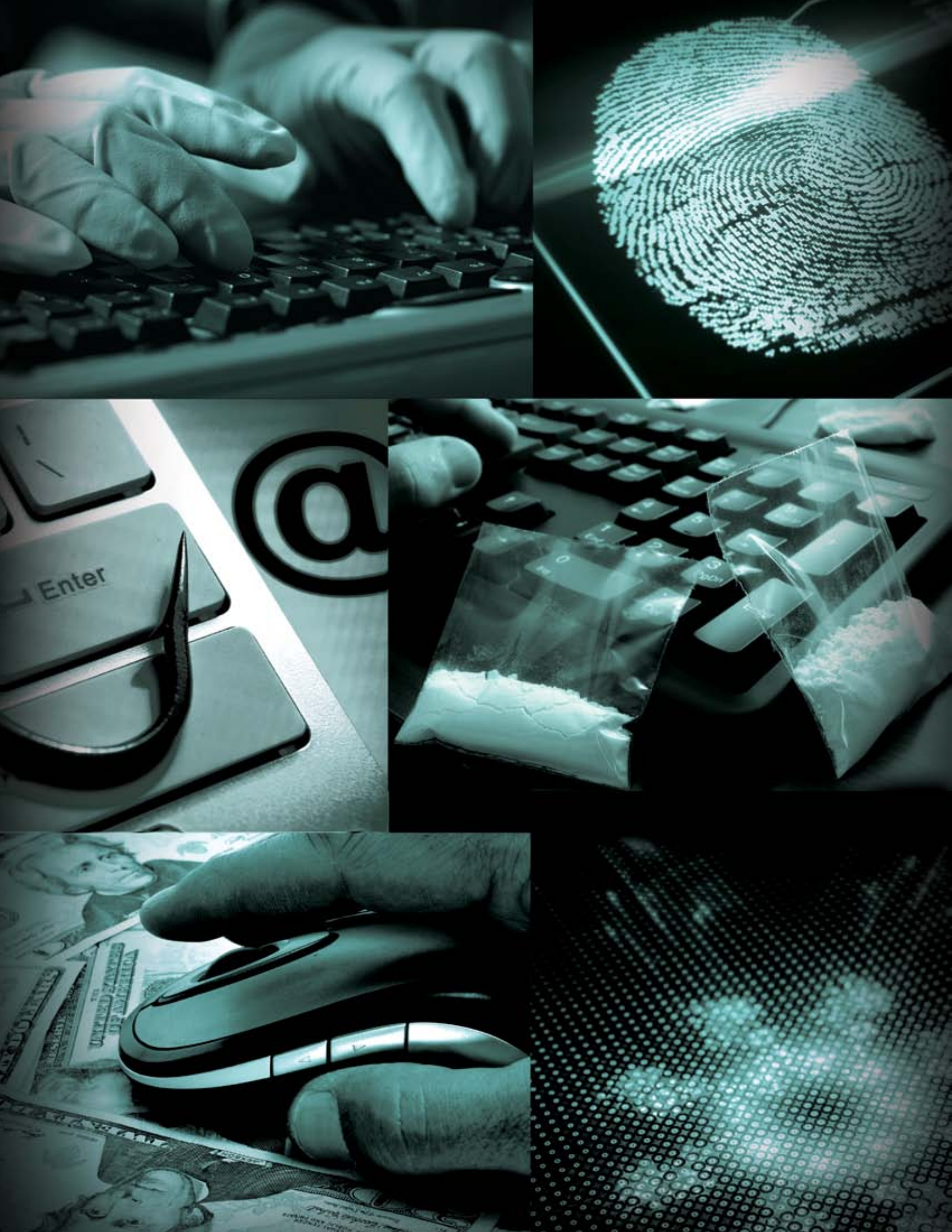
These categories are examined in this report through examples and law enforcement case studies involving recent cybercrime threats. The report concludes with three key observations:

- **Technology creates new opportunities for criminals.** Online markets and Internet-facing devices provide the same opportunities and benefits for serious and organized criminal networks as they do for legitimate businesses.

- **Cybercrime is expanding.** Once considered the domain of criminals with specialized skills, cybercrime activities have expanded to other offenders as the requisite know-how becomes more accessible.

- **Cybercrime requires new ways of policing.** The criminal exploitation of new and emerging technologies - such as cloud computing and social media platforms, anonymous online networks and virtual currency schemes – requires new policing measures to keep pace in a digital era.

This report and future versions will inform Canadians of criminal threats and trends in cyberspace, and law enforcement efforts to combat them.


Enter

Inside the Report

DEFINING CYBERCRIME FROM A LAW ENFORCEMENT PERSPECTIVE

The RCMP generally interprets cybercrime to be any crime where *cyber* - the Internet and information technologies, such as computers, tablets, personal digital assistants or mobile devices - has a substantial role in the commission of a criminal offence. It includes technically advanced crimes that exploit vulnerabilities found in digital technologies. It also includes more traditional crimes that take on new shapes in cyberspace. Viewing cybercrime through this broad lens is vital in determining the best response, whether involving law enforcement or other cyber security measures.

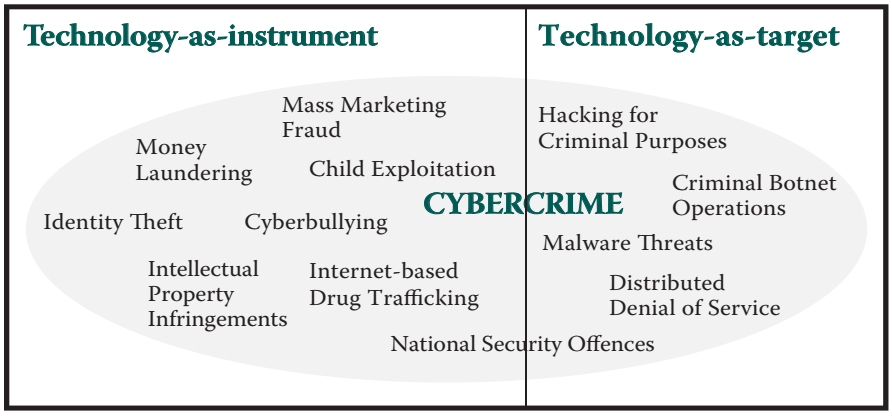
Cybercrime may be broken into two categories:

- **technology-as-target:** criminal offences targeting computers and other information technologies, such as those involving the unauthorized use of computers or mischief in relation to data, and;
- **technology-as-instrument**: criminal offences where the Internet and information technologies are instrumental in the commission of a crime, such as those involving fraud, identity theft, intellectual property infringements, money laundering, drug trafficking, human trafficking, organized crime activities, child sexual exploitation or cyber bullying.

These categories account for the widespread criminal exploitation of new and emerging technologies. They enable the RCMP to address serious and organized crimes where offenders use technology to extend the reach of their traditional activities, and to identify new criminal activities that unfold in tandem with technological advancements. These categories also separate cybercrime from 'incidental' uses of technology in crime, where the Internet and related technologies play an ancillary role and do not materially alter the respective criminal activity (e.g. use of text messaging to sell drugs, or conducting open source research on the Internet to plan a robbery).

Technology-as-target and *technology-as-instrument* cybercrimes should not be interpreted as mutually exclusive. In many cases, the more technically advanced forms of cybercrime (hacking into a computer to steal personal data or remotely using keystroke loggers to capture financial credentials) may be instrumental in furthering the reach of more traditional criminal offences (using the same personal or financial data to facilitate mass-marketing fraud or extortion). These definitions will be elaborated below through recent examples of investigations and enforcement actions.

Figure 1: cybercrime categories



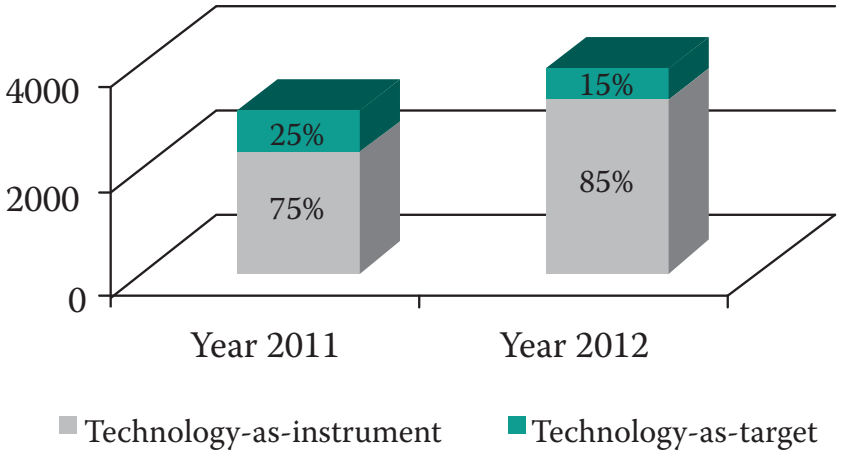
Cybercrime is on the rise

Cybercrime is difficult to measure and often goes unreported to law enforcement agencies. However, RCMP statistics suggest that cybercrime continues to grow in Canada. In 2012, the RCMP received nearly 4,000 reported incidents of cybercrime: an increase of over 800 reported incidents from 2011. In both years, *technology-as-instrument* cybercrimes accounted for the majority of reported incidents.

These figures only tell part of the story. Other studies and reports show increases in select aspects of Canada's cybercrime environment. For example, in 2013 the Canadian Anti-Fraud Centre (CAFC) received over 16,000 complaints of cyber-related fraud (email and website scams), accounting for more than $29 million in reported losses.

However, cybercrime does not have to be financially motivated to have a devastating impact on victims. Online child sexual exploitation is a prime example. In 2013 alone, the RCMP National Child Exploitation Coordination Centre (NCECC) received over 9,000 reported incidents and requests for assistance from law enforcement and other partners concerning online child sexual exploitation.

Table 1: number of RCMP-reported cybercrime incidents in 2011 and 2012



CANADIAN ANTI-FRAUD CENTRE

The Canadian Anti-Fraud Centre (CAFC) is Canada's trusted source for reporting and mitigating online mass marketing fraud. It is a partnership among the RCMP, Ontario Provincial Police (OPP) and the Competition Bureau: **www.antifraudcentre-centreantifraude.ca**.

NATIONAL CHILD EXPLOITATION COORDINATION CENTRE

The RCMP National Child Exploitation Coordination Centre (NCECC) works with law enforcement partners across Canada and internationally to combat the online sexual exploitation of children. The NCECC also works closely with the Canadian Centre for Child Protection, a charitable organization that operates Canada's national tipline for reporting the online sexual exploitation of children: **www.cybertip.ca**.

CYBERCRIME THREATS AND CASE STUDIES

The following examples and case studies show the range of offences that fall under the RCMP's definition of cybercrime, and how governments, businesses and citizens can be victimized by cybercrime in different ways.

Technology-as-target cybercrimes

Technology-as-target cybercrimes are considered to be 'pure' forms of cybercrime as they did not exist prior to the advent of the Internet and related technologies. These crimes apply to Canada's *Criminal Code* offences involving the unauthorized use of computers and mischief in relation to data. They center on exploiting software or other information technology vulnerabilities for criminal purposes. Criminals find ways to compromise these technologies and obtain, alter or outright destroy personal or sensitive information, or remotely access and infiltrate computers, system networks or mobile devices for a variety of illegal activities.

Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) attacks inundate targeted computer servers or websites with false requests until an online service is disrupted and rendered inoperable, which may in turn prevent legitimate consumers from using the targeted service. The impact of a DDoS attack can range from temporary inconveniences to more noticeable effects, including lost business opportunities and reputational damages from service disruption. These attacks can be politically, ideologically or financially motivated, or simply used to challenge and disrupt a public or private organization. These criminal activities may also link to 'insider' threats.

Cyber insider threat

An insider threat is a malicious and often criminal threat to a public or private organization that comes from someone inside the organization, such as an employee or contractor, who is attempting to disrupt the activities of the organization. While not unique to cybercrime, insider threats involving unauthorized computer use or data mischief represent a growing risk to organizations that rely on the Internet, networked systems and related technologies. These threats extend the ways in which insiders can steal from an organization or commit criminal breach of trust.

CASE 1: DDOS ATTACK ON GOVERNMENT WEBSITE

In 2012, the RCMP investigated a DDoS attack originating from offices belonging to the House of Commons against the government of Québec's portal website 'www.gouv.qc.ca,' which caused the website to be inaccessible for over two days. During the criminal investigation, the RCMP used login names, building access records, surveillance images and digital evidence (seized computer equipment) to identify the suspect, a government network administrator who gained administrative privileges to 'www.gouv.qc.ca' to upload malware. In 2013, the suspect was convicted of two counts of unauthorized use of computers and one count of mischief, and sentenced to house arrest.

Cyber-related insider threats are of significant concern to critical infrastructure organizations (like those in government, transportation, finance, manufacturing or energy industries) and others that use information technology systems. Through inside and direct access, criminals can bypass 'air gaps' – computer security layers that isolate networks from unsecure networks – and directly compromise a secure computer network, such as installing a virus on a network via a USB device.

Case 1 represents both a DDoS attack and an insider threat to government computer networks and related information technology systems.

Criminal botnet operations

A 'botnet' involves a network of computers that are remotely controlled by a command-and-control server. Botnets may be used to deploy malware and infect thousands or potentially millions of computers for various criminal purposes, such as distributing a malware program for data access, screen and password captures, or keystroke loggers to obtain personal and financial credentials.

In many cases, victims are unaware that their business or personal computers may be part of a botnet operation and that their data may be siphoned for criminal purposes. Without knowing, an individual could activate malware on a computer by clicking on a seemingly benign email or website link, in turn giving some code-scripted form of control to a botnet operation (such as access to online bank account passwords through keystroke monitoring and recording). These threats not only involve 'pure' cybercrime offences, but may also be used to facilitate more traditional crimes, such as fraud and identity theft. Operation Clean Slate (*case 2*) is an example of a recent law enforcement initiative against an international criminal botnet operation.

CASE 2: OPERATION CLEAN SLATE

In 2013, the United States Federal Bureau of Investigation (FBI) advised the RCMP of Canadian IP addresses that were suspected of command and control operations for a network of infected computers ('botnet'). Known as Citadel, these botnets installed malware on computers to steal personal and financial data and targeted major financial institutions in Canada and internationally, costing an estimated $500 million in global economic losses. This specific type of malware enabled criminals to remotely access business and personal computers to steal online banking data, credit card information and other credentials. In response, the RCMP seized more than 80 physical servers to help mitigate the spread of this criminal botnet operation. The FBI and its international law enforcement and government partners worked closely with information technology and financial service industries to successfully disrupt more than 1,400 botnet components of the Citadel malware threat, which freed more than an estimated two million infected computers globally.

Technology-as-instrument cybercrimes

Pure cybercrimes often involve the theft and exchange of personal or financial information, which extends to *technology-as-instrument* cybercrimes. Other crimes

involve the use of the Internet and information technologies in different ways, and take on a new magnitude in cyberspace. The examples and case studies below illustrate the range of *technology-as-instrument* cybercrime activities.

Carding crimes

Carding crimes are offences in which the Internet is used to traffic and exploit personal and financial data and share cybercrime techniques, such as the online buying and selling of stolen identity and counterfeit documents, credit card and bank account information, or criminal hacking tools. Carding crimes and others like it show how pure cybercrimes can be instrumental in facilitating and altering the scope of more traditional criminal offences. For example, a criminal may gain unauthorized access to a computer database to steal personally identifiable information and credit card numbers. In turn, the criminal may use anonymous online forums, many of which are not detectable through online search engines, to exchange this information for illegitimate purposes.

Operation Card Shop (*case 3*) provides a glimpse at an international law enforcement operation against carding crimes.

Online mass-marketing fraud and ransomware

Links between pure and instrumental cybercrimes are arguably most common in fraud. The Internet has transformed this long standing criminal offence to the extent where 'mass marketing' is now linked to many types of fraud. Internet-based mass marketing frauds such as phishing emails, lottery scams, '419' scams and romance scams are used to deceive victims and steal personal identifiers for a variety of financially motivated criminal purposes. These scams easily target large populations across multiple jurisdictions in a far more ubiquitous, anonymous and efficient manner when compared to similar offline crimes. One of these fraud-based cybercrimes is exemplified through 'ransomware.' Ransomware scams involve a type of malware that locks a computer and its data content and uses social engineering tactics, such as threats, to coerce victims into paying fees for regained computer access. Recent threats involving ransomware scams are described in *case 4*.

CASE 3: OPERATION CARD SHOP

In 2010, the RCMP assisted the FBI and other international law enforcement partners to investigate carding offences (e.g. online buying and selling of personal and financial data) and detect individuals who were involved in associated cybercrime activity. The two-year operation led to an international law enforcement takedown of identified suspects and revealed suspected criminal activity in Canada. The RCMP assisted the takedown with coordinated operations in British Columbia, Alberta and Ontario, leading to the arrest of one individual who waived extradition to the United States.

The operation spanned eight countries, led to 24 arrests and subsequent convictions, and prevented an estimated $205 million in global economic losses by notifying credit card providers of over 400,000 compromised credit and debit cards, and over 40 public and private sector organizations of breaches to their networks.

CASE 4: RANSOMWARE SCAMS

In 2012, the Canadian Anti-Fraud Centre (CAFC) received complaints from Canadians who were seeing fraudulent pop-up messages on their computers, stating that their "operating system is locked due to the violation of the laws of Canada," including false accusations of sharing online child pornography and sending spam messages with terrorist motives.

The illegitimate messages were designed to appear as instructions from the RCMP or the Canadian Security Intelligence Service (CSIS) advising individuals to pay $100 in electronic currency to unlock their computers. In 2012, the RCMP and the CAFC received hundreds of reports from Canadians who encountered the ransomware pop-up message, which was linked to downloaded malware from infected websites and fraudulent emails. The RCMP used its website to inform the public of this malware threat and to encourage affected consumers to report suspected incidents to the CAFC. Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) also provided a cyber security bulletin, which included computer recovery procedures for these malware infections.

These threats continue to affect Canadians. In 2013, the CAFC received over 2,800 reports from individuals who came across the latest variant of ransomware - Cryptolocker - accounting for over $15,000 in reported losses that were paid by victims in an attempt to regain computer access. Cryptolocker is an executable file that appears as a PDF image and is activated when victims unsuspectingly click on the image. The virus encrypts computer files and folders, which may be decrypted when the victim makes an online payment to the responsible fraudster for regained access (decryption key). The RCMP, the CAFC and government partners continue to mitigate ransomware threats through prevention tactics and other cyber security measures.

Organized crime and the Internet

The Internet and related technologies have created new opportunities, new markets and new delivery methods for criminal transactions that are not possible in the 'real' world. For drugs, contrabands and other types of criminal trafficking, these technologies have created a virtual storefront presence where criminal networks can efficiently and anonymously buy, sell and exchange criminal products and services on an unprecedented scale. In some cases, these cybercrime threats are also associated with money laundering and organized criminal activity. Through the Internet and online currency schemes, criminal money transfers originating from Canada can be electronically routed through foreign jurisdictions with weaker safeguards to more effectively conceal illicit proceeds and simplify offshore banking. Money launderers can also collude and exploit legitimate online services, such as auctions or online gambling, to hide criminal proceeds by buying and selling fictitious items or by masking such proceeds as legitimate gambling profits. *Case 5* illustrates the rising threat of

online money laundering and its links to organized crime.

Online child sexual exploitation

The Internet has transformed and exacerbated criminal activity involving the sexual exploitation of children. In cyberspace, criminals hide their true identities through pseudonyms and share child sexual exploitation material through private websites and online bulletin boards. Operation Snapshot (*case 6*) illustrates the harmful and ubiquitous nature of online child sexual exploitation and the role of law enforcement.

CASE 5: ORGANIZED CRIME, MONEY LAUNDERING AND THE INTERNET

In 2012, the RCMP and Combined Forces Special Enforcement Unit partners discovered an organized crime group that was suspected of using an off-shore gambling website, Platinum Sports Book.com, to launder proceeds of crime generated in Canada and make money through illegal gambling. Over a year-long operation, the RCMP connected Canada-based activity with the gambling website. The website was host to thousands of gamblers whose wagers allegedly resulted in millions of dollars in profit for organized crime.

The operation resulted in a takedown and dismantling of the gaming enterprise in 2013, in which over 30 individuals were arrested and charged with numerous gaming offences (e.g. participating in or contributing to an activity of a criminal organization, keeping a common betting house, and conspiracy), and the seizure of more than $3 million.

CASE 6: OPERATION SNAPSHOT

In 2012, the RCMP took part in Operation Snapshot, a multi-agency investigation that focused on identifying high-risk offenders who were in possession of or distributing child sexual exploitation images across peer-to-peer file sharing networks. The demanding investigation involved the seizure of over 100 computers and hard drives that required digital forensic analysis, along with hundreds of thousands of child sexual exploitation images. The investigation led to the rescue of one child and the arrest of more than 15 individuals in connection with various sexually-based offences (e.g. accessing child pornography, possession of child pornography, distribution of child pornography, making child pornography, Internet luring).

The multi-agency operation continued in 2013 with Operation Snapshot II, where investigations had two key priorities: identify and rescue children who were victims of sexual exploitation, and identify and charge high-risk offenders who collect, possess or distribute online child sexual exploitation material. These investigations led to the rescue of two children and the arrest of 22 individuals from across Atlantic Canada who were suspected of collecting, possessing and distributing online child sexual exploitation material.

EVOLVING CYBERCRIME THREATS

Cybercrime threats are becoming more sophisticated as criminals continue to exploit information technologies, which present significant challenges for law enforcement to detect and attribute. The following are some of the evolving cybercrimes that may form the basis of future RCMP reports.

Darknets

Darknets are online file sharing networks that provide users with anonymity through encryption and other cyber security technologies. They enable criminals to broker their illegal goods and services on the Internet and avoid detection through anonymous online networks. These networks attract criminal activity by concealing online transactions, such as the online buying and selling of illegal drugs, pirated media, counterfeit goods and other illicit products.

Cybercrime-as-a-service

Through darknets and other online forums, criminals can purchase or rent cybercrime tools, services and supporting infrastructure with relative ease. This service-based online market enables more criminals to take part in technically advanced cybercrimes, such as criminal operations involving DDoS attacks or malware distribution via botnets. The online availability of such tools and services means that more criminals can outsource their cybercrime operations in part or in whole.

Malware targeting mobile platforms

The popularity and interconnectedness of mobile devices, such as smartphones and tablets, have made them an attractive target for criminal exploitation. Malware variants are increasingly being developed to target vulnerabilities found in mobile operating systems. Mobile device features, such as text messaging and downloadable applications, are used to deploy malware and gain remote and unauthorized access to mobile platforms for various illicit purposes, such as stealing personal data and obtaining GPS coordinates.

Virtual currency schemes

Virtual currency schemes, such as Bitcoins, are used by criminals to launder their proceeds online (money laundering). These schemes provide organized crime networks with new means to hide their earnings from law enforcement. The criminal use of virtual currencies is often associated with darknets, in which virtual currencies and anonymous online networks are used to obtain payments for illegal goods and services and launder revenue associated with criminal transactions.

Cyber-facilitated stock market manipulation

Cybercrime extends to online stock market manipulation schemes. Criminals use social engineering techniques to obtain personal credentials, or deploy malware programs such as keystroke loggers, to 'hijack' live-trading user accounts and manipulate the share price of targeted securities. Other cybercrime threats, such as DDoS attacks, also impact capital markets by undermining investor confidence in online services and affecting targeted stock market valuations.

Cybercrime threats to industrial control systems

Industrial control systems, such as Supervisory Control and Data Acquisition (SCADA) systems, are used to monitor and control industrial processes, such as those involved in power plants or electrical grids. These systems may include Internet-facing components, potentially leaving them vulnerable to DDoS attacks or other cybercrime threats involving malware programs. The impact of these threats to critical infrastructure may vary, ranging from industrial espionage, to data extraction and theft of intellectual property or trade secrets, to more disruptive tactics involving system compromises.

Conclusion: key observations

This report provides a primer on cybercrime threats and trends that harm Canada's public organizations, business interests and citizens in real and tangible ways. While far from exhaustive, it highlights a number of issues in the cybercrime environment to demonstrate the range of offences in Canada's *Criminal Code* that fall under cybercrime. It concludes with three general observations.

Technology creates new opportunities for criminals
The Internet and related technologies have reshaped Canada's society and economy; they have also changed Canada's criminal landscape. Online markets and Internet-facing devices provide the same opportunities and benefits for serious and organized criminal networks as they do for legitimate businesses. Through information technologies, criminals are expanding their reach to commit entirely new crimes, and old crimes in new ways.

Cybercrime is expanding
Once considered the domain of criminals with specialized skills, cybercrime activities have expanded to other offenders as the requisite know-how becomes more accessible. Widely available and ready-made malware tools – which can be bought, sold or exchanged online - provide criminals with new and simplified ways to steal personal information and cause monetary losses to Canadian businesses and citizens. Cyber technologies are also used for other harmful purposes, such as online child sexual exploitation and the rising prevalence of cyber bullying.

Cybercrime requires new ways of policing
The criminal exploitation of new and emerging technologies - such as cloud computing and social media platforms, anonymous online networks and virtual currency schemes – requires new policing measures to keep pace in a digital era. Criminal activities in cyberspace are complex and often transnational in character, where potential evidence is transient and spread across multiple jurisdictions. Addressing these challenges requires broad-based domestic and international law enforcement cooperation, engagement with public and private sector organizations, and integrating new technical skills and tools with traditional policing measures.

The RCMP has a broad mandate when it comes to investigating and apprehending criminals in the online world, or otherwise disrupting cybercrime activity. To improve its capabilities in the cyber realm, the RCMP is developing a strategy to better combat cybercrime in concert with its domestic and international partners. The strategy is scheduled for completion in 2014 and will complement *Canada's Cyber Security Strategy* to help keep Canadians secure online.