CACP

EXECUTIVE GLOBAL STUDIES PROGRAM

PROGRAMME D'ÉTUDES INTERNATIONALES POUR CADRES SUPÉRIEURS

ACCP

CYBER CRIME:
LET'S GET ON WITH IT

COHORT 2015 FINAL PRESENTATION

May 29, 2015

PRESENTATION OUTLINE

- Cohort Research Theme
- The Problem: A snapshot baseline assessment
- Research Objective / Statement
- Our Dimensions
- Our Findings
- Our Recommendations

COHORT RESEARCH THEME

Global and Domestic Cyber Warfare: Canadian Policing Responses to Crime, Victimization and National Security

“It is a topic that challenges the traditional skills, capacities, roles and response patterns of policing, and in this, policing is not alone. As the tableau of crime-fighting agencies and other governmental and non-governmental actors continues to evolve, and as the demand for specialized investigative methods and skills continues to expand, the need for a coherent national response is an emerging priority for police leaders.” (emphasis added)

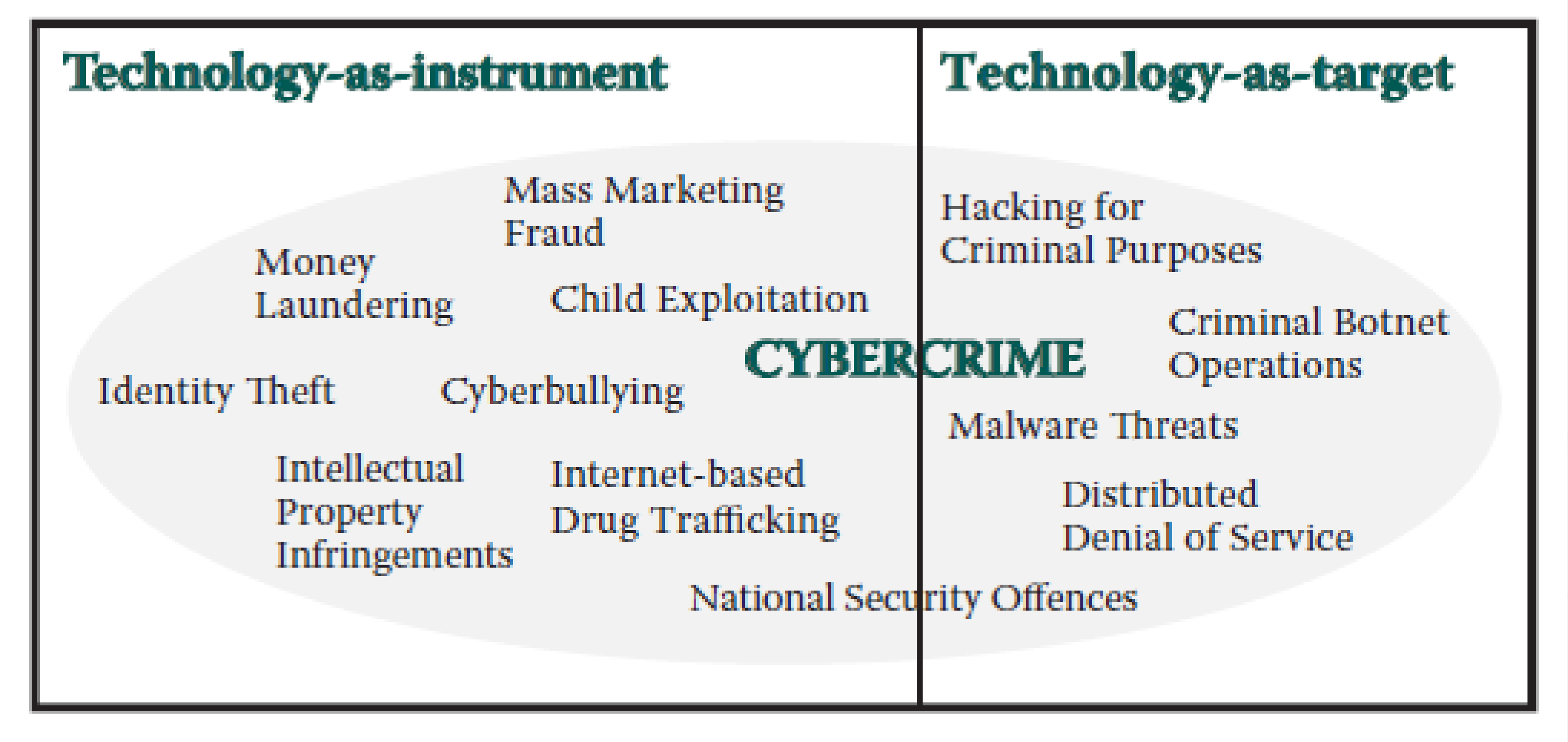
OVERALL RESEARCH OBJECTIVE

Current empirical evidence strongly suggests that solutions to cyber-based victimization demand effective collaboration among multiple actors;

All levels of policing share unique responsibilities to protect citizens and to uphold the rule of law;

To illuminate a way forward for Canada, our study will examine approaches in certain other countries to identify the most effective roles for police within a collaborative framework.

The Problem: A snapshot


Technology-as-instrument
Technology-as-target
Mass Marketing Fraud
Money Laundering
Child Exploitation
Identity Theft
Cyberbullying
Intellectual Property Infringements
Internet-based Drug Trafficking
CYBERCRIME
Hacking for Criminal Purposes
Criminal Botnet Operations
Malware Threats
Distributed Denial of Service
National Security Offences

The cyber universe is ill-defined but expanding, touching most areas of life and types of criminality.

Source: RCMP.

The Problem: A snapshot

50% **OF ONLINE ADULTS HAVE BEEN VICTIMS OF CYBERCRIME AND / OR NEGATIVE ONLINE SITUATIONS IN THE PAST YEAR**

1M+ ADULTS BECOME CYBERCRIME VICTIMS EVERY DAY - THAT'S 12 VICTIMS PER SECOND

$113 BILLION USD

TOTAL DIRECT GLOBAL COSTS IN JUST 12 MONTHS

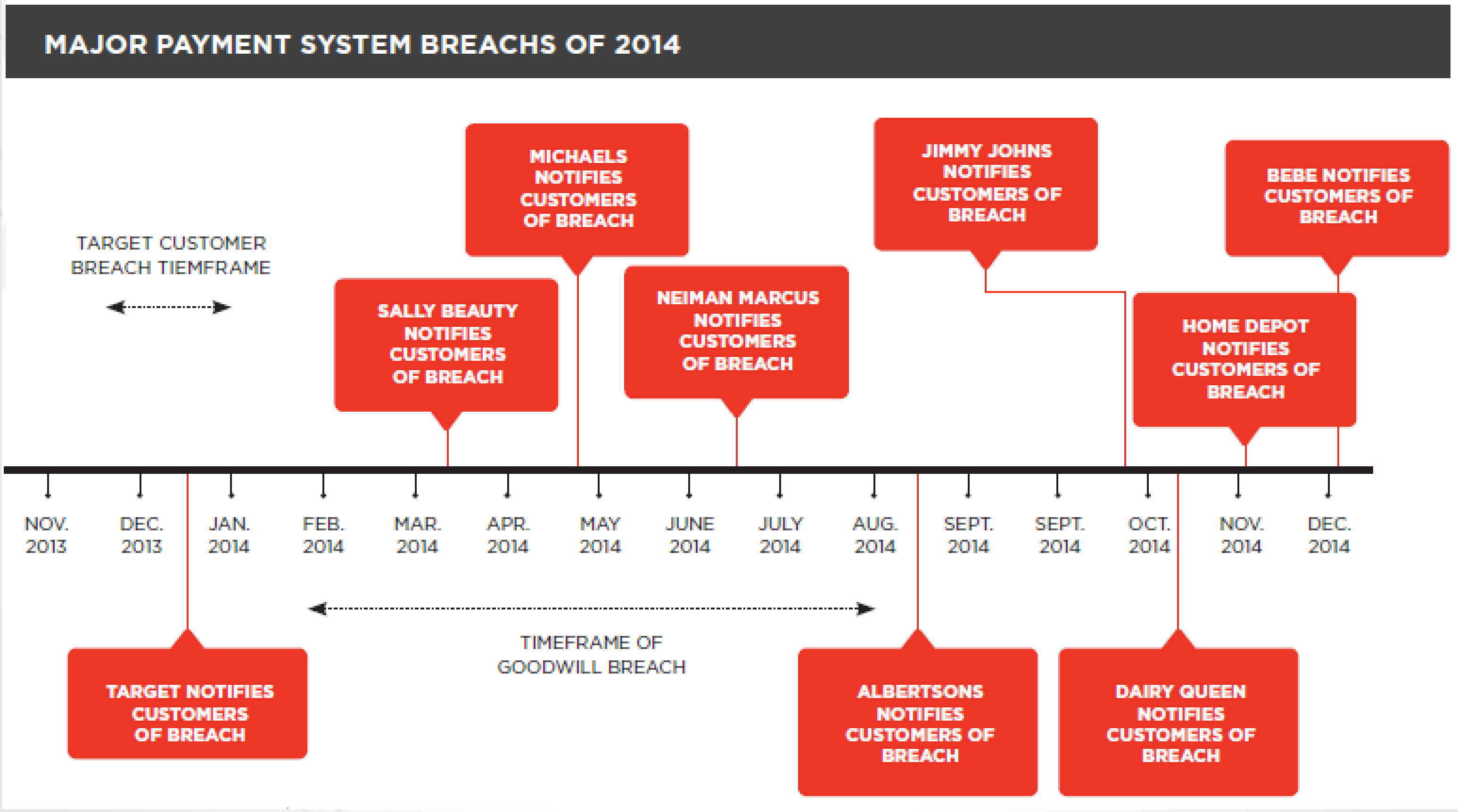
Source: Norton by Symantec. Based on 2013, survey of 13,022 adults in 24 countries aged 18-64 years.

The Problem: A snapshot

Gameover Zeus, a complex botnet, is estimated to have done **$100 million** in financial damage.

Source: CrowdStrike Global Threat Intel Report 2014.

The Problem: A snapshot



MAJOR PAYMENT SYSTEM BREACHS OF 2014

TARGET CUSTOMER BREACH TIEMFRAME

TARGET NOTIFIES CUSTOMERS OF BREACH

SALLY BEAUTY NOTIFIES CUSTOMERS OF BREACH

MICHAELS NOTIFIES CUSTOMERS OF BREACH

NEIMAN MARCUS NOTIFIES CUSTOMERS OF BREACH

TIMEFRAME OF GOODWILL BREACH

JIMMY JOHNS NOTIFIES CUSTOMERS OF BREACH

ALBERTSONS NOTIFIES CUSTOMERS OF BREACH

HOME DEPOT NOTIFIES CUSTOMERS OF BREACH

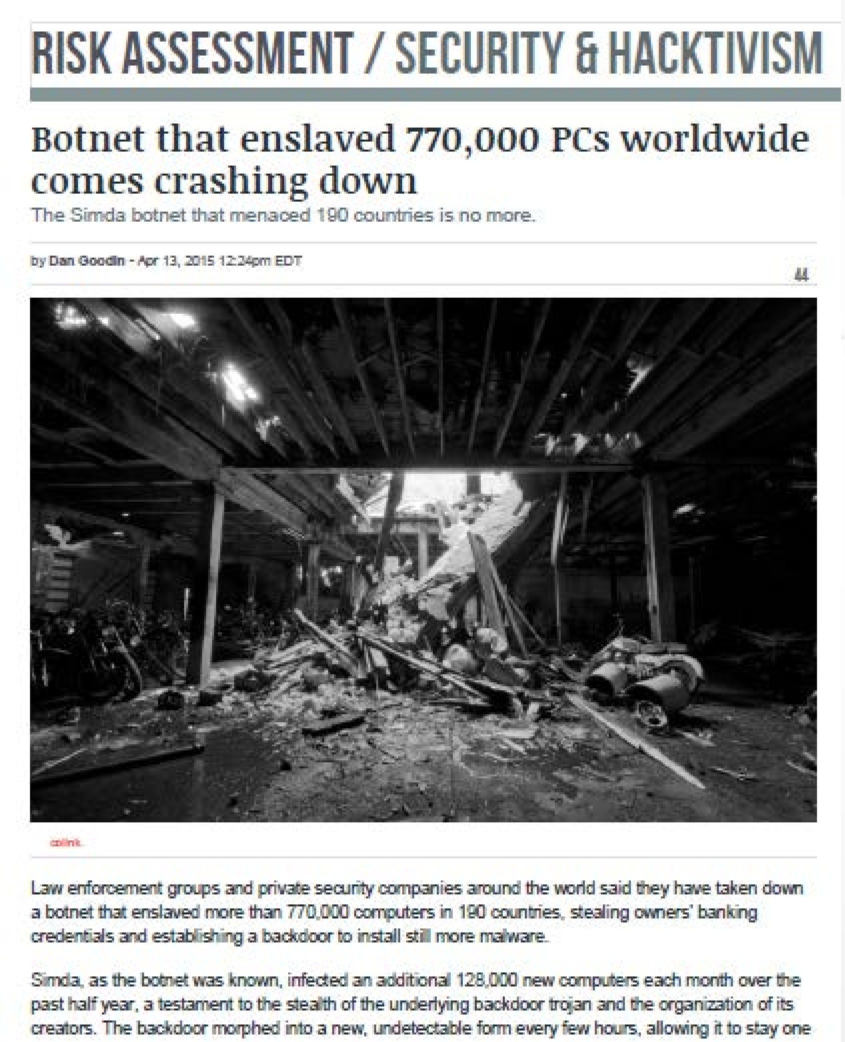
DAIRY QUEEN NOTIFIES CUSTOMERS OF BREACH

BEBE NOTIFIES CUSTOMERS OF BREACH

The Target breach alone compromised **40 million** credit card numbers and personal information of **70 million** individuals. More should be expected.

Source: CrowdStrike Global Threat Intel Report 2014.

The Problem: A snapshot



RISK ASSESSMENT / SECURITY & HACKTIVISM

Botnet that enslaved 770,000 PCs worldwide comes crashing down

The Simda botnet that menaced 190 countries is no more.

by Dan Goodin - Apr 13, 2015 12:24pm EDT

44

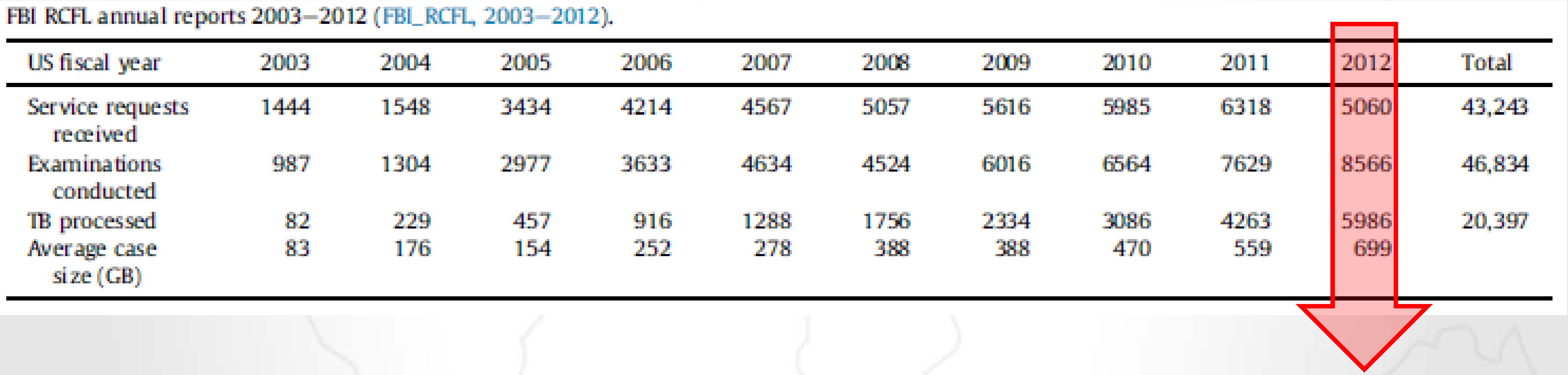
colink.

Law enforcement groups and private security companies around the world said they have taken down a botnet that enslaved more than 770,000 computers in 190 countries, stealing owners' banking credentials and establishing a backdoor to install still more malware.

Simda, as the botnet was known, infected an additional 128,000 new computers each month over the past half year, a testament to the stealth of the underlying backdoor trojan and the organization of its creators. The backdoor morphed into a new, undetectable form every few hours, allowing it to stay one

Source: Ars Technica, http://arstechnica.com/security/2015/04/botnet-that-enslaved-770000-pcs-worldwide-comes-crashing-down/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+arstechnica%2Findex+%28Ars+Technica+-+All+content%29

The Problem: A snapshot



FBI RCFL annual reports 2003–2012 (FBI_RCFL, 2003–2012).

US fiscal year	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	Total
Service requests received	1444	1548	3434	4214	4567	5057	5616	5985	6318	5060	43,243
Examinations conducted	987	1304	2977	3633	4634	4524	6016	6564	7629	8566	46,834
TB processed	82	229	457	916	1288	1756	2334	3086	4263	5986	20,397
Average case size (GB)	83	176	154	252	278	388	388	470	559	699	

Since 2003…

3.5x growth in requests

8.6x growth in examinations

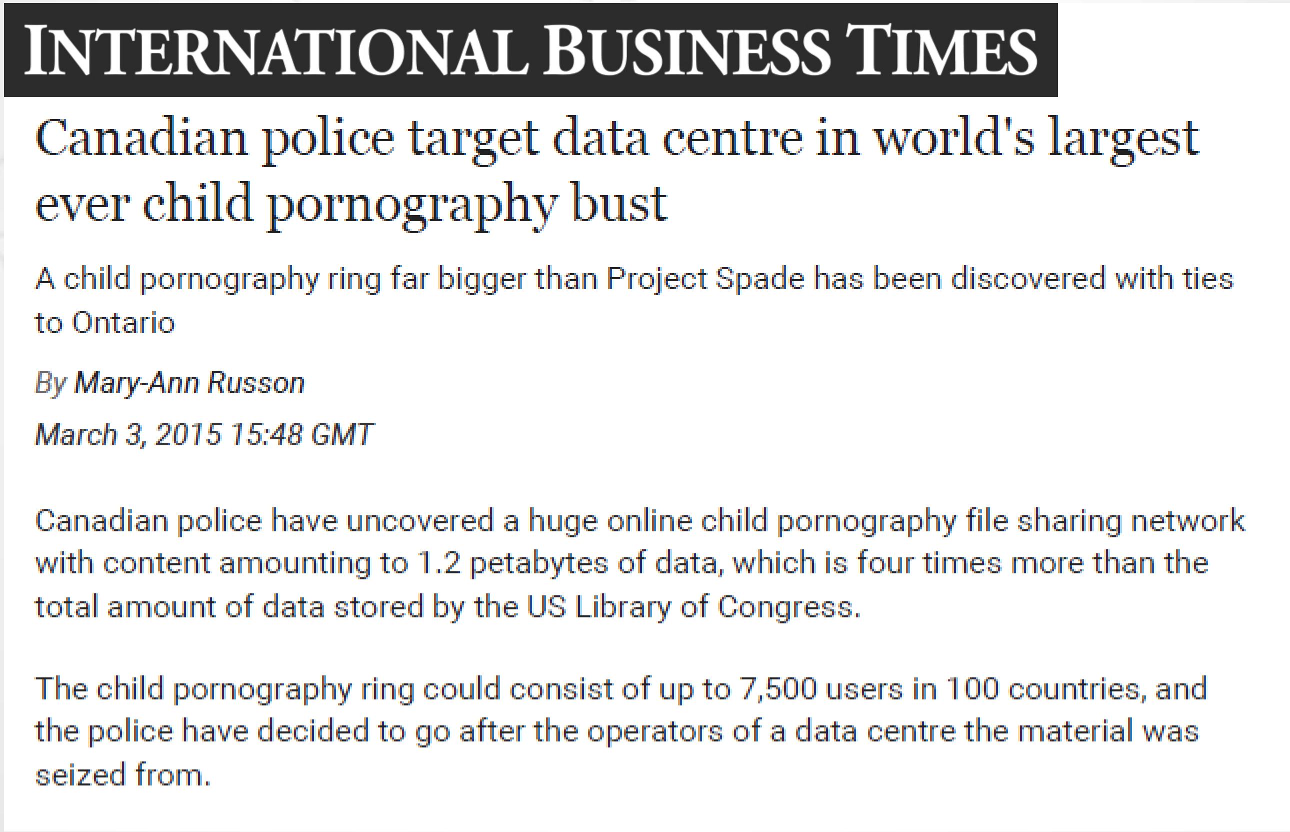
51.9x growth in data processed

8.4x growth in avg case size

The challenge of digital forensics is growing increasingly difficult as demand for seized media exploitation grows almost exponentially

Source: http://dx.doi.org/10.1016/j.diin.2014.09.002

The Problem: A snapshot



INTERNATIONAL BUSINESS TIMES

Canadian police target data centre in world's largest ever child pornography bust

A child pornography ring far bigger than Project Spade has been discovered with ties to Ontario

By Mary-Ann Russon

March 3, 2015 15:48 GMT

Canadian police have uncovered a huge online child pornography file sharing network with content amounting to 1.2 petabytes of data, which is four times more than the total amount of data stored by the US Library of Congress.

The child pornography ring could consist of up to 7,500 users in 100 countries, and the police have decided to go after the operators of a data centre the material was seized from.

Source: http://www.ibtimes.co.uk/canadian-police-target-data-centre-worlds-largest-ever-child-pornography-bust-1490293

The Problem: A snapshot

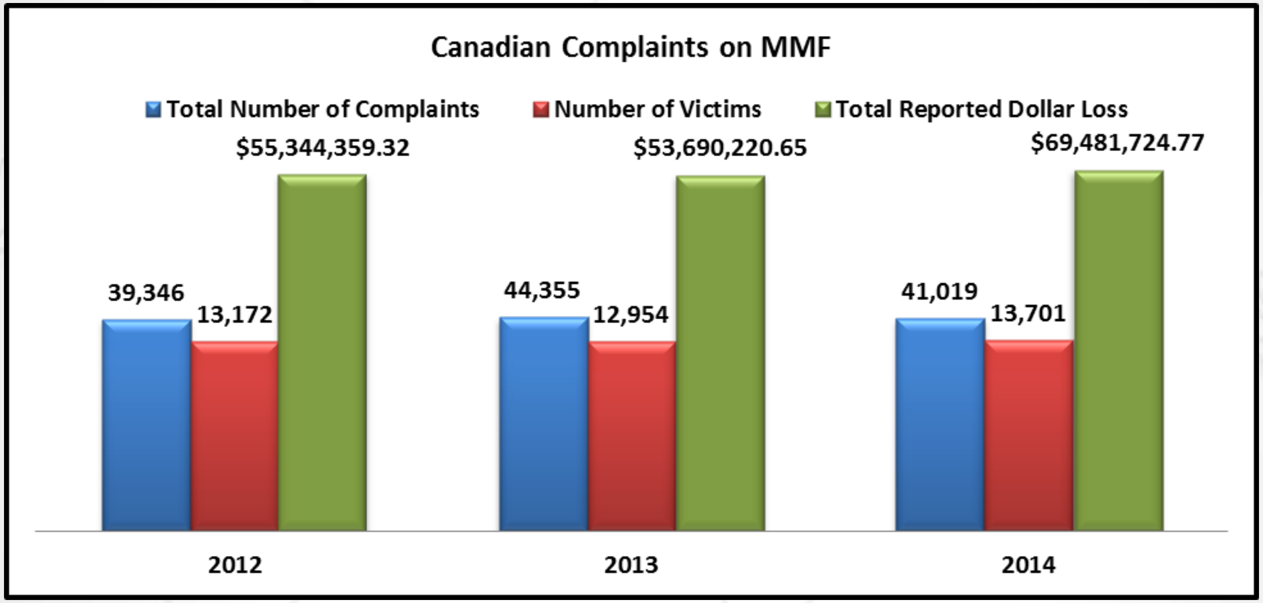
“It is expected that **by 2020 between 26 and 30 billion** uniquely identifiable embedded computing devices are interconnected within the existing internet infrastructure.”

This Internet of Things (IoT) is here / on the horizon.

The revolution is just getting started.

Source: “The internet of things: Interconnected digital dust,” *Digital Investigation* 11 (2014) 141-142**,** http://dx.doi.org/10.1016/j.diin.2014.09.002

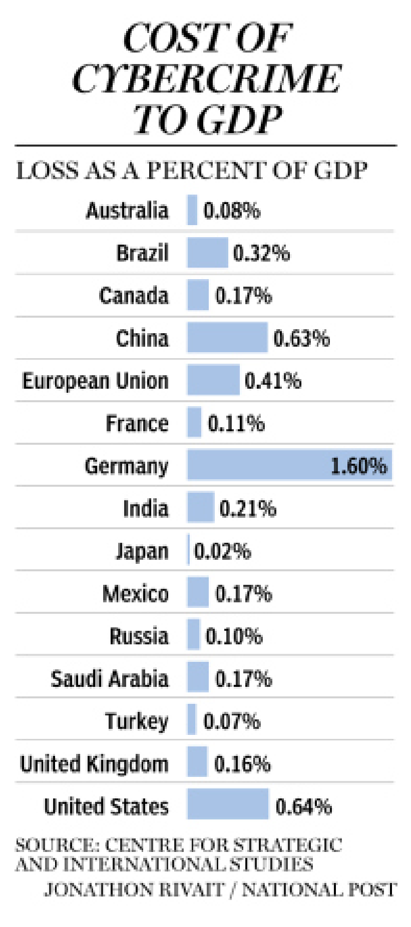
The Problem: A snapshot



In the first **six weeks of 2015,** The City of London Police have suspended more than 2,000 websites selling fake luxury goods.

Source: Canadian Anti-Fraud Centre, Annual Report. **Source:** http://www.wired.co.uk/news/archive/2015-02/13/counterfeit-goods-websites-suspended

The Problem: A snapshot



Source: http://business.financialpost.com/2014/06/09/grasping-in-the-dark-how-canadas-undercounting-of-cybercrime-costs-may-be-leaving-us-vulnerable/?__lsa=9963-5513#__federated=1

The Problem: A snapshot

9,084 incidents reported to police in 2012 according to Statistics Canada

Source: Statscan 2012

Summary of Current Efforts (Public Sector)

GLOBAL

- Five Eyes Law Enforcement Group
- INTERPOL – Singapore
  - Global Digital Crime Centre
- Europol - European Cyber Crime Centre (EC3)
  - Joint Cyber Action TF (J-CAT)
  - Cyborg (Cybercrime associated with Internet and ICT)
  - Terminal (Payment Card Fraud)
  - Twins (Child Exploitation on the Internet)
- G7 Roma-Lyon Group
- FBI led International Cyber Crime Task Force (ICCTF) – formerly known as Operation Clean Slate
- FBI-National Cyber Forensic and Training Alliance (NCFTA)-led taskforce

NATIONAL

- RCMP Technical Investigative Services – HQ Ottawa
- RCMP National Intelligence Coordination Centre (NICC) cyber team – HQ Ottawa
- RCMP National Coordination Centres (Critical Infrastructure, Child Exploitation, Human Trafficking)
- CACP e-Crime / Private Sector Liaison Committees
- Canadian Anti Fraud Centre (RCMP, OPP, Competition Bureau)
- NCFTA – Montreal
- Other non-Law Enforcement Cyber Teams [CSE, CSIS, DND, IC, CRTC, Competition Bureau, Public Safety-led Canadian Cyber Incident Response Centre (CCIRC)]

PROVINCIAL AND MUNICIPAL

- Integrated Child Exploitation Units
- Various municipal Technical Investigative Units
- Various units dedicated to investigate cyber as an instrument of crime (ie. Cyber bullying, human trafficking, fraud, etc.)
- RCMP Divisional Investigative Technical Crime Units

Knock knock!

INITIAL TAKEAWAYS

- Effort ongoing, disconnected. The best info / intel rests with private industry, emphasizing the need for trust.

- Defining victims, offenders, locations of offences is a challenge.

- Focus on *genuine* collaboration and *fulsome* information sharing and *tangible* coordination validated. This requires a paradigm shift in thinking.

- The pace of change is staggering and we need to think about the future.

- Don’t reinvent the wheel and further fragment the system. Our proposal must be relevant and pragmatic for Canada understanding that the challenge won’t be fixed overnight.

- No one has solved cyber.

Cohort Baseline Assessment

This activity faces 8 enduring challenges in the Canadian context:

1. Definition
2. Capacity
3. Competency
4. Coordination
5. Jurisdiction
6. Legislation
7. Dialogue
8. Future

TEAM 1: UK/SPAIN

- London Metropolitan Police
- City of London Police
- West Midlands Police (ROCU)
- National Crime Agency
- Crown Prosecution Service
- Cabinet Office
- College of Policing
- KPMG

Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.

- The UK Cyber Security Strategy

Key Takeaways:

- **Significant investment in a national cyber crime strategy driven by the national risk assessment.**
- **Balanced strategy based on the 4 P's.**
- **Lead to a restructuring of their enforcement and response capacities.**
- **The strategy has ownership at a high level with national accountability.**

"Making the UK one of the safest places to do business online…"

TEAM 1: UK / SPAIN

- Spanish National Centre of Excellence (University of Madrid)
- Civil Guard
- National Department of Security

Roger / Nick / Dave / Mark

The National Cyber Security Strategy in Spain consists of five chapters.

1. Cyber Space and its Security
2. Purpose and Guiding Principles of Cyber Security
3. Cyber Security Objectives in Detail
4. Lines of Action of National Cyber Security
5. National Cyber Security System Structure

Key Takeaways:

- *National government has invested in a cyber crime strategy.*
- *Law enforcement is connected to the national strategy.*
- *Academia supports capacity and capability within the national strategy.*

TEAM 2: NETHERLANDS / GERMANY / FRANCE

Ministry of Security and Justice Law Enforcement Directorate
National Coordinator for Security and Counterterrorism
Hague Security Delta
National Cyber Security Centre (NCSC)
European Cybercrime Centre (EC3)

Cyber Intelligence Unit
Federal Office for Information Security (BSI)
Cyber Analysis and Defence Department
Essen Police Services
Lower Saxony Police Services
German Competence Centre against Cyber Crime (G4C).

Prefet, Charge de la Lutte Contre les Cybermenaces
Charge Geographique, Amerique du Nord, Direction de la Coopération Internationale

TEAM 2: NETHERLANDS / GERMANY / FRANCE

KEY TAKEAWAYS

- vast and significant impact
- common systems approach
- close relationships between police and industry
- need for victims to report cybercrimes to law enforcement
- need to improve information sharing
- specialization of police and judiciary to investigate and prosecute cybercrime
- lack of cybercrime awareness among the population
- need for specialized police training
- need for all stakeholders to work together
- no common metrics to measure cybercrime

TEAM 3: AUSTRALIA / NEW ZEALAND (1)

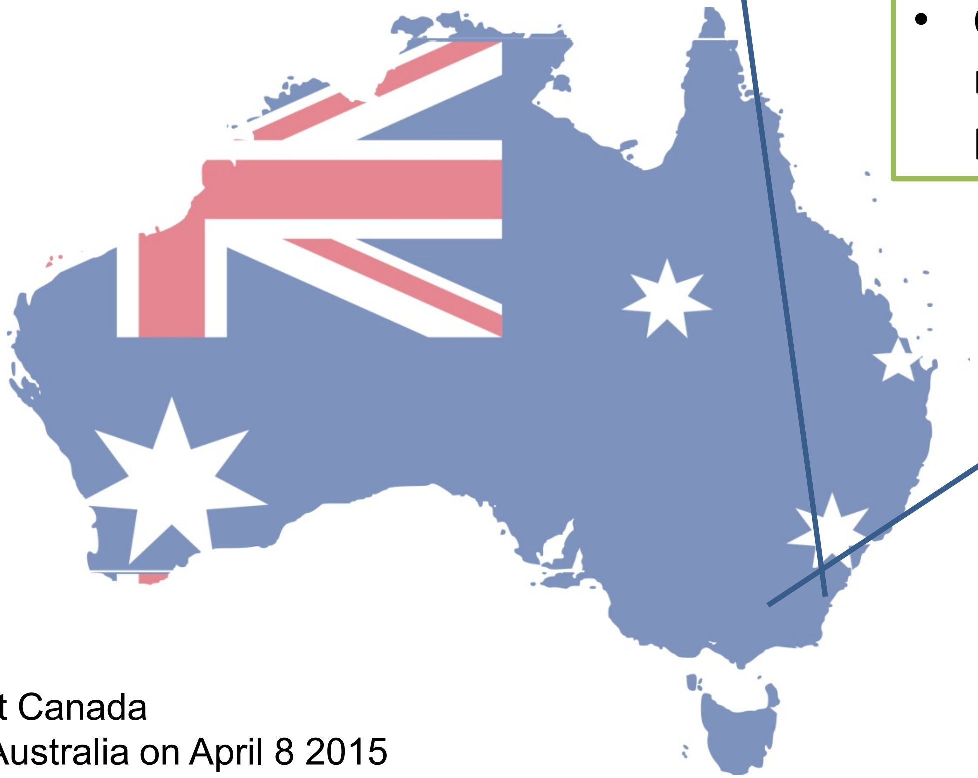
Sydney, AUS

10 - 13 Apr

- New South Wales Police

Key Points:

- Holistic approach
- ACORN (Australian Cybercrime On-Line Reporting Network)
- Improved information sharing
- Training is required
- Clear delineation of roles and responsibilities (governance and prescribed standards ANZPAA)



Canberra, AUS

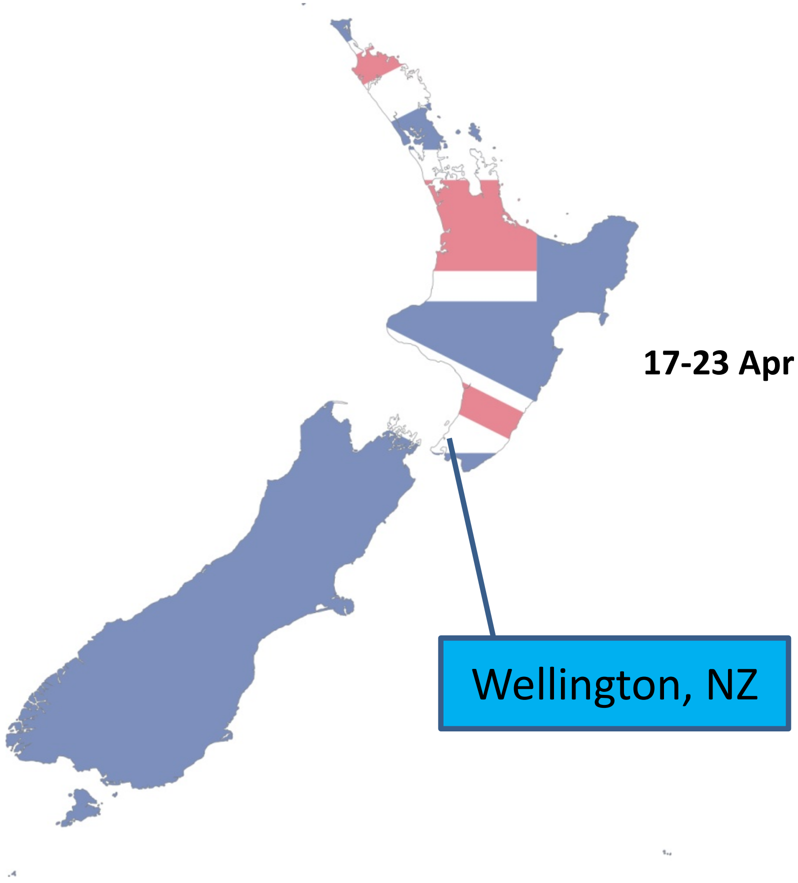
13 - 17 Apr

- Australian Federal Police
- Australian Crime Commission
- Charles Sturt University
- Australian National University
- Australian Cyber Security Center

Left Canada
to Australia on April 8 2015

Arrive 10 April 2015

TEAM 3: AUSTRALIA / NEW ZEALAND (2)



Wellington New Zealand

- New Zealand Police Service
- National Cyber Intelligence Office
- National Cyber Policy Office
- New Zealand Internet Task Force
- New Zealand Financial Crime Management (ANZ Bank)
- Victoria University
- NZ Ministry of Foreign Affairs and Trade

Key Points:

- Prevention focussed with community awareness being key
- Mandatory Disclosure is being sought
- Online Reporting mechanism (ORB)
- Majority of offenders reside outside of New Zealand.

TEAM 4: INDIA / SINGAPORE

KEY TAKEAWAYS

Information sharing remains a challenge

Border-based solutions for a Borderless crime (lack of coordination)

Collaboration with Private Sector

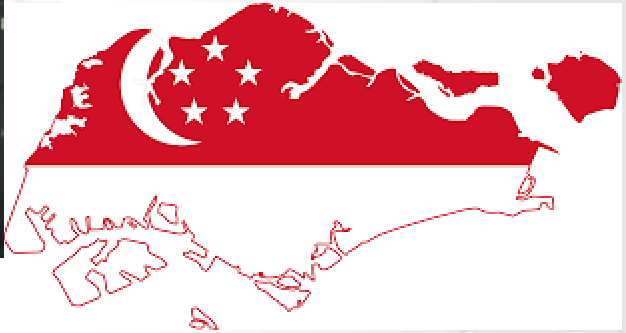
Training is key

Public Awareness

Future is bleak

SINGAPORE

- **Excellence** in approach
- **Innovation**, massive internet penetration
- Strong **collaboration** between state and industry



- **Interpol** Global Complex for Innovation
- **Microsoft** Global Cybercrime Center
- **Police Force Tech Crime Branch**
- **Attorny General's Chambers**

Team of Tomorrow

Bernadine / MC / Shahin / Liam

TEAM 4: INDIA / SINGAPORE

INDIA

- Rapidly growing economy, massive IT sector
- Cybercrime up by 80%
- States within federal system

NEW DELHI, TRIVENDRUM AND BANGALURU

- **Central Bureau of Investigation** -- Cybercrime Cells / Academy
- **Center for Cyber-Victim Counseling**
- **Kerala Police Cyberdome**
- **CERT-N**
- **NASSCOM/DSCI**
- **Lawyers and Acadamia**

KEY TAKEAWAYS

Information sharing remains a challenge

Social Media is challenging

Border-based solutions for a Borderless crime (lack of coordination)

Collaboration with Private Sector

Training is key

Public Awareness/education

Future is bleak

Research

HOW OUR THINKING EVOLVED

THE PUBLIC HEALTH MODEL

4Ps

G4C

THE CRIME MODEL

THE WAY FORWARD

OUR RECOMMENDATIONS

1. Mainstream “cyber”

2. Increase community awareness and victim support

3. Extend trust and collaboration beyond law enforcement

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

5. Enhance capability and capacity of the judicial system

6. Advocate for certain legislative and regulatory changes

MAINSTREAM CYBER

- A paradigm shift is needed.
- The definition isn't that important.
- The label "Cyber" conflates what's just crime in 2015.
- Build up investigative capability in general units
- Law enforcement needs to train the public facing aspects of their services to recognize crime online as crime and encourage reporting

"…Its like salt in your food. It is in everything"

- *Insp. Gupta*
  Central Bureau of Investigation Academy
  India

INCREASE COMMUNITY AWARENESS AND VICTIM SUPPORT

- Provide support to victims

- Get to the kids, and get to them early and often

- Create online tools to enable reporting to police

- Don’t own the problem. Signpost to existing initiatives like getcybersafe.ca and cyber bullying.

- CACP should consider a “cyber safety” equivalent to National Prescription Drug Drop-off day.

EXTEND TRUST AND COLLABORATION BEYOND LAW ENFORCEMENT

- A robust model collaboration for across sectors is necessary.

- Co-location in an integrated framework with formal appropriate information sharing protocols is ideal.
    - We can work within current frameworks. We must accept a level of risk to encourage thoughtful information sharing.

- We should leverage / restructure / realign existing structures and initiative into a consolidated approach

- We need to move quickly to stop further fragmentation of the Canadian response.

ESTABLISH COORDINATION MECHANISMS

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

- Online crime challenges current deployment models / authorities / jurisdictions.

- A F/P/T conversation is needed to overcome the constitutional fragmentation of Canadian policing

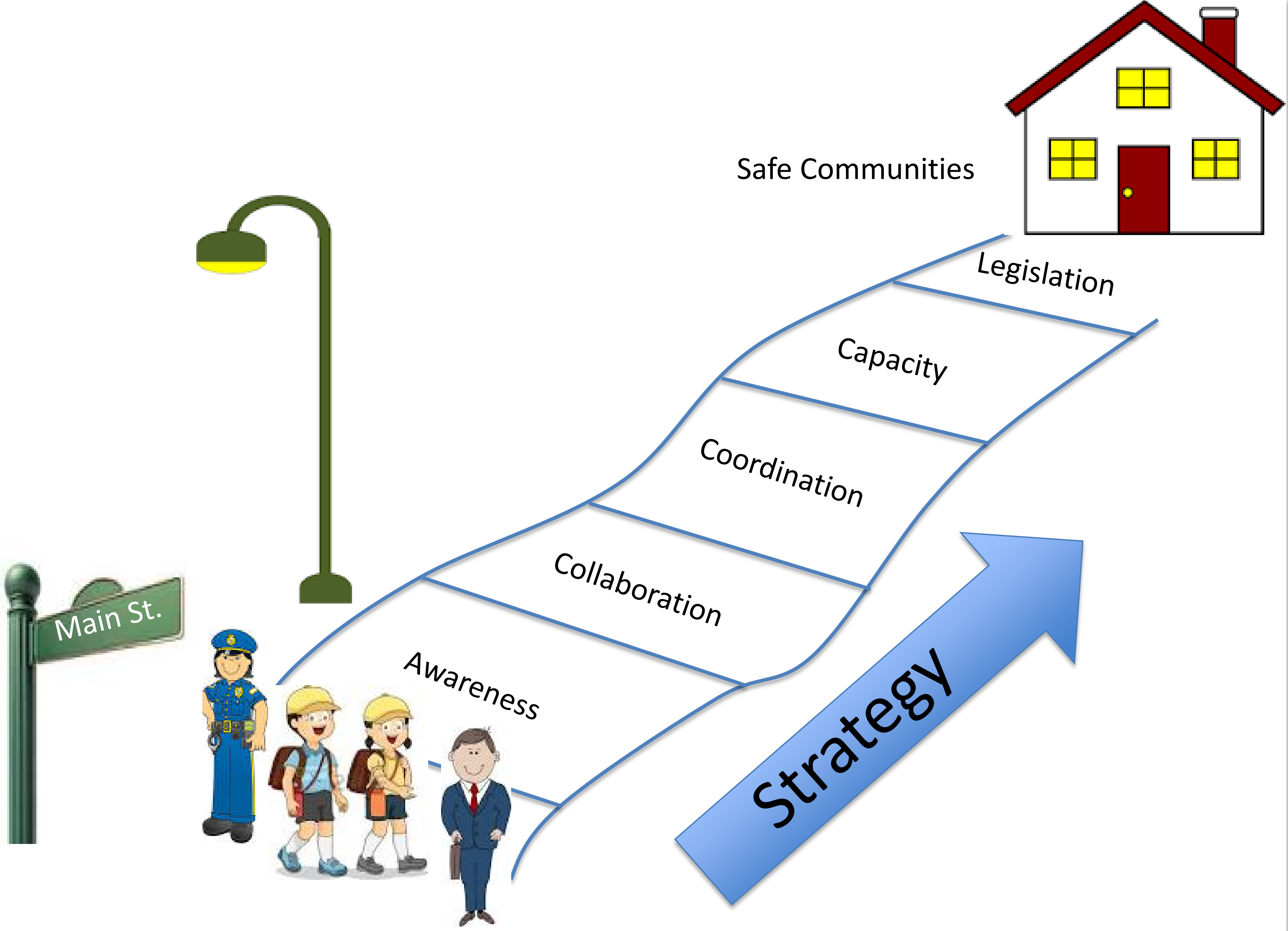
- A Canadian Charter (akin to the Budapest Convention) to align Canadian policing and its governing authorities for the 21st century could be useful

ENHANCE THE JUDICIAL SYSTEM

- We need to address capability and capacity of law enforcement and the judicial system
- Regional cyber crime investigative teams are needed
- Cyber/digital basics should be included in all cadet training
- Additional specialized / advanced in-service training too
- Educate Crowns and encourage specialized prosecutors
- Tools for digital forensics need to be pushed to the frontline
- Non-traditional recruiting and retention models should be examined

ADVOCATE FOR LEGISLATIVE CHANGE

- Data preservation standards are required (1 yr minimum)
- Powers to enable domestic production orders for foreign data would greatly streamline a range of investigations
- The MLAT process is broken
- Extra-territoriality of attacks on vital cyber systems
- Access to encrypted data



Safe Communities

Legislation

Capacity

Coordination

Collaboration

Awareness

Strategy