VULNERABLE CONNECTIONS

The Expert Panel on Public Safety in the Digital Age

CCA | CAC

All people in Canada are **digital-by-default**—whether they are online or not. While the internet and its associated technologies provide many benefits and are essential to everyday life, they also enable malicious actors to target people and communities. *Vulnerable Connections* details a range of cyber-enabled harms, the challenges facing policymaking and enforcement of existing rules, and opportunities for improving digital public safety.

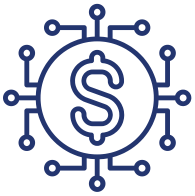
WHAT ARE "CYBER-ENABLED HARMS"?

Cyber-enabled harms are activities in which technology is used as an instrument to inflict damages on individuals and communities. The number of cyber-related crimes has risen in Canada each year since 2014. However, not all online harms constitute illegal acts—and, of those that are criminal, many are not reported.

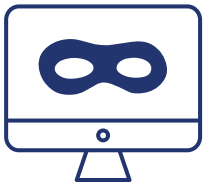
Examples of cyber-enabled harms:

- Harassment
- Fraud
- Hate propaganda
- Child sexual abuse material

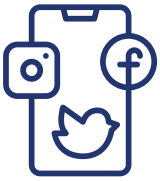
HOW DO DIGITAL TECHNOLOGIES ENABLE HARM?



Cryptocurrencies and crowdfunding sites are largely decentralized, and have little oversight.



The Dark Web and virtual private networks provide high levels of anonymity.



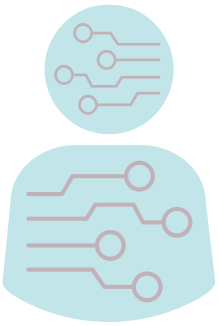
Harmful content spreads easily via social media, and platforms face moderation challenges.

PRIVACY, SECURITY, AND THE FUTURE

There is a complex interplay among privacy, security, and human rights in the context of digital technologies, complicating efforts to regulate against cyber-harms. However, efforts to protect individuals against cyber-enabled harms need not minimize privacy protections. **Privacy is an essential component of security.** In the Panel's view, security and privacy can be mutually reinforcing.

RESPONDING TO CYBER-ENABLED HARMS

The criminalization of harmful online activities is not always appropriate, and may not be effective. **Victims of such harms may prefer other, non-criminal avenues for recourse**—including tort law, Quebec civil law, privacy legislation, and anti-spamming legislation. Responses may also focus on the removal of harmful content, or on prevention efforts.



LAW ENFORCEMENT CHALLENGES

The abilities of law enforcement to respond to cyber-enabled crimes are limited by a range of factors, including:

Outdated organizational structures

A growing volume of digital evidence

Insufficient digital capacity

Cross-jurisdictional cooperation challenges

A COLLECTIVE EFFORT

A healthy online ecosystem requires the participation of:

Governments

Law enforcement

Civil society

Private-sector organizations

Social media platforms