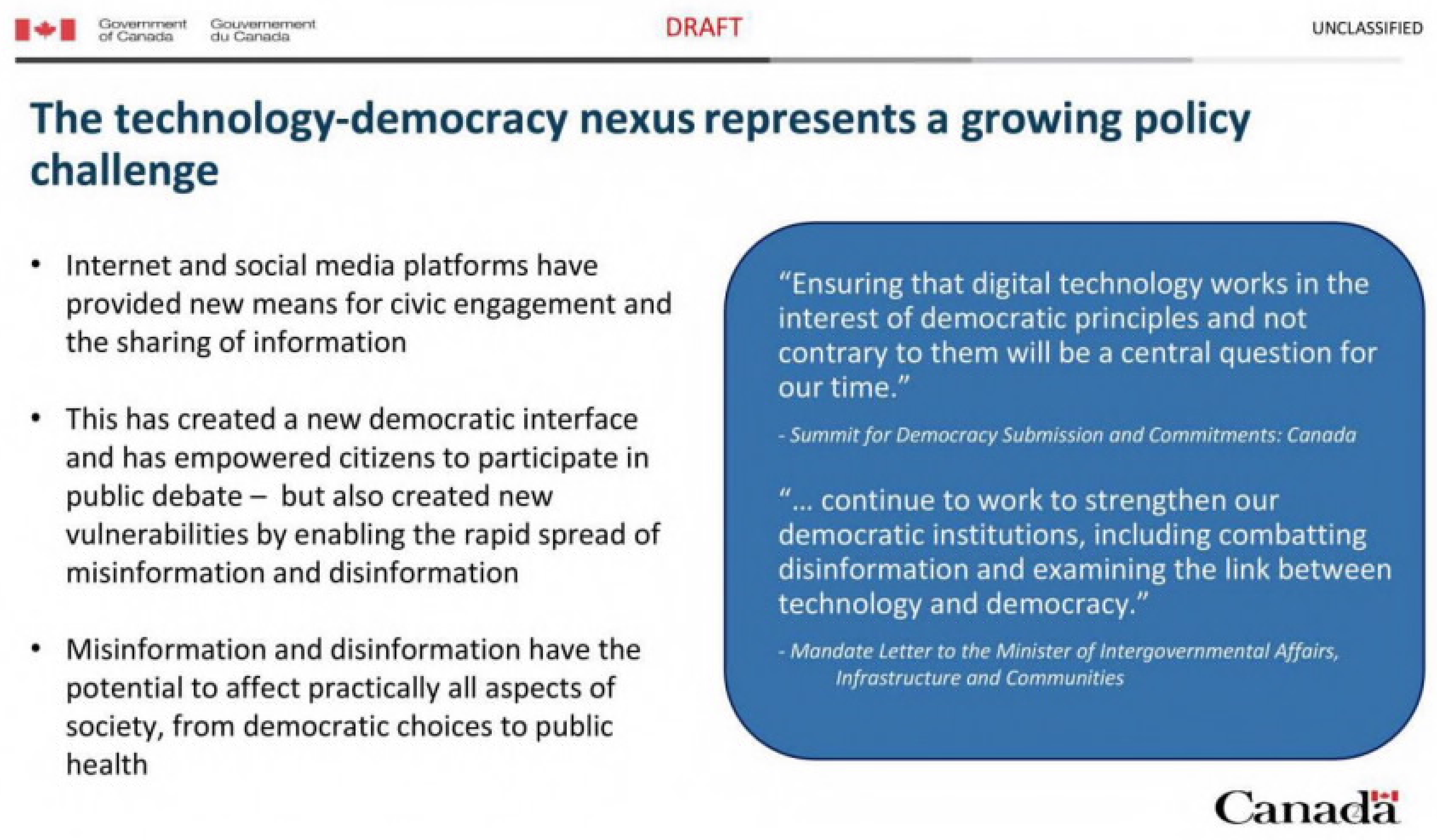
Government of Canada Gouvernement du Canada

DRAFT

UNCLASSIFIED

Combating Disinformation through Civil Society Partnership

Building an Online Integrity Network



Government of Canada Gouvernement du Canada

DRAFT

UNCLASSIFIED

The technology-democracy nexus represents a growing policy challenge

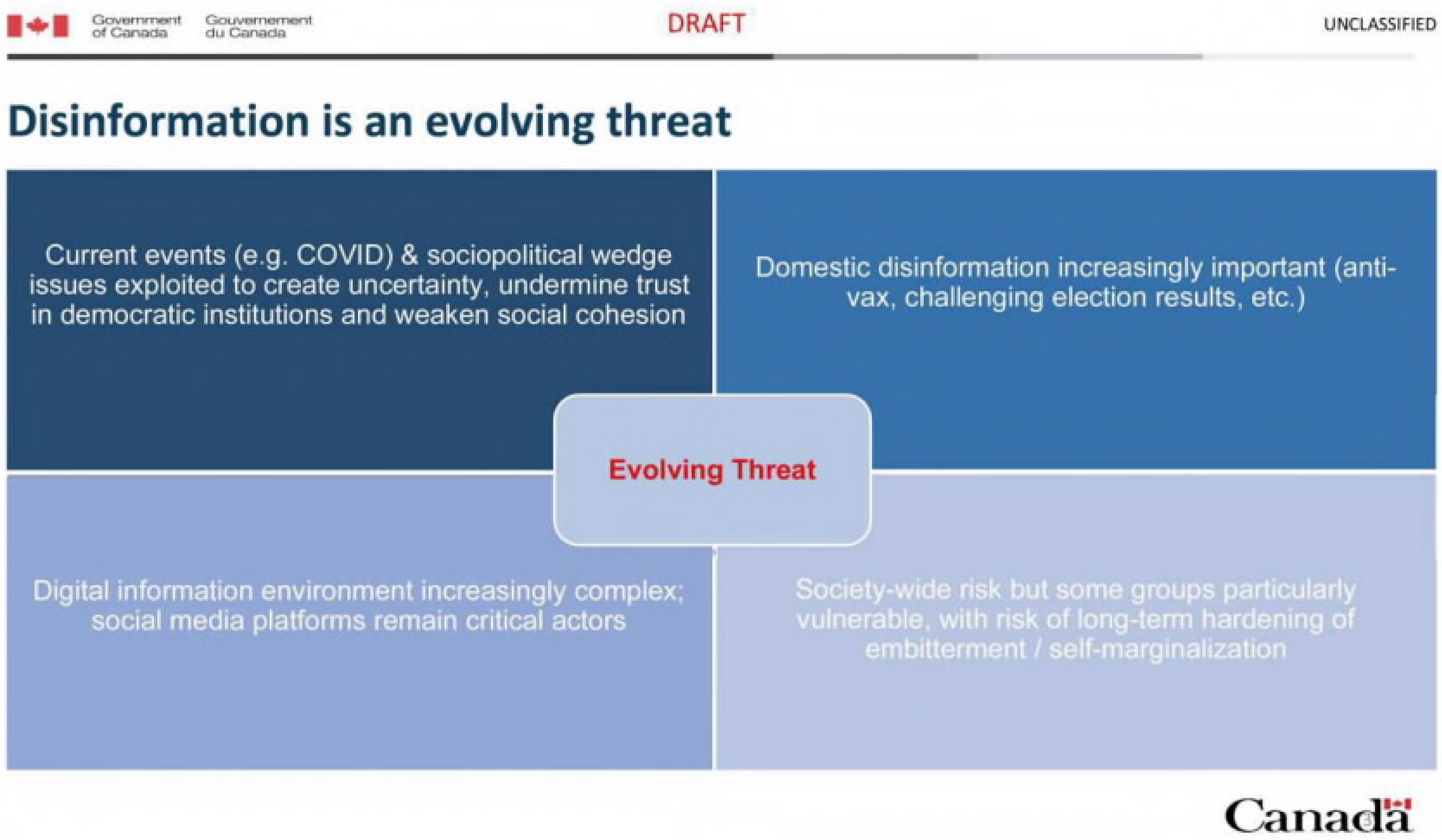
- Internet and social media platforms have provided new means for civic engagement and the sharing of information

- This has created a new democratic interface and has empowered citizens to participate in public debate – but also created new vulnerabilities by enabling the rapid spread of misinformation and disinformation

- Misinformation and disinformation have the potential to affect practically all aspects of society, from democratic choices to public health

> "Ensuring that digital technology works in the interest of democratic principles and not contrary to them will be a central question for our time."
>
> *- Summit for Democracy Submission and Commitments: Canada*
>
> "… continue to work to strengthen our democratic institutions, including combatting disinformation and examining the link between technology and democracy."
>
> *- Mandate Letter to the Minister of Intergovernmental Affairs, Infrastructure and Communities*

Canada



Government of Canada Gouvernement du Canada

DRAFT

UNCLASSIFIED

Disinformation is an evolving threat

Current events (e.g. COVID) & sociopolitical wedge issues exploited to create uncertainty, undermine trust in democratic institutions and weaken social cohesion

Domestic disinformation increasingly important (anti-vax, challenging election results, etc.)

Evolving Threat

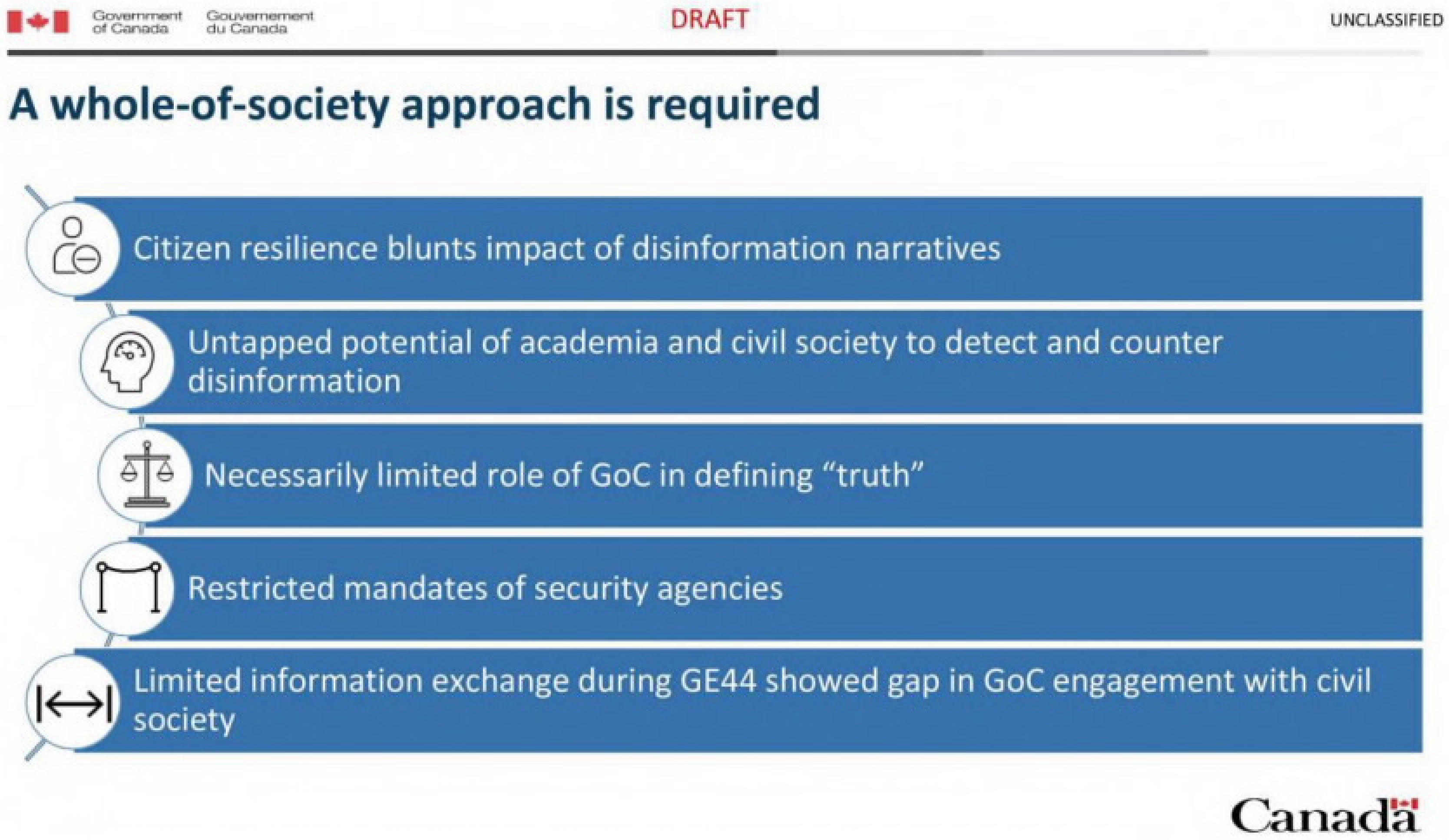
Digital information environment increasingly complex; social media platforms remain critical actors

Society-wide risk but some groups particularly vulnerable, with risk of long-term hardening of embitterment / self-marginalization

Canada

Government of Canada action is needed

- Disinformation threat is evolving more rapidly than the information ecosystem's ability to adapt organically, with risk of significant long-term effects
- Vibrant debate is at the core of the democratic system
- Support to basic democratic institutions (including confidence therein) strengthens all of society



Government of Canada Gouvernement du Canada

DRAFT

UNCLASSIFIED

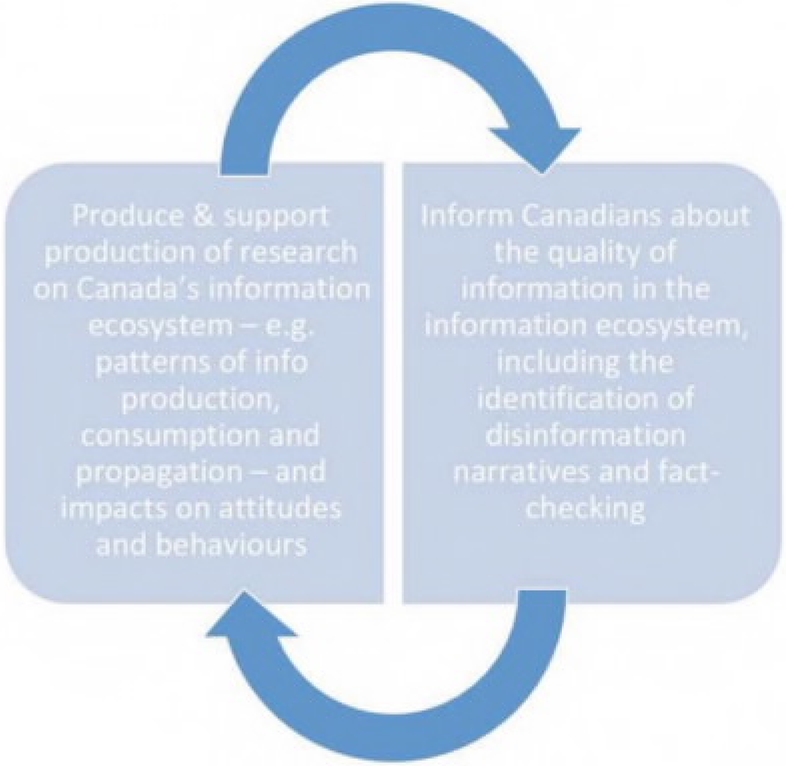
A whole-of-society approach is required

- Citizen resilience blunts impact of disinformation narratives
- Untapped potential of academia and civil society to detect and counter disinformation
- Necessarily limited role of GoC in defining “truth”
- Restricted mandates of security agencies
- Limited information exchange during GE44 showed gap in GoC engagement with civil society

Canada

The Online Integrity Network

- A **novel partnership between government, academia and civil society** to support public resilience to disinformation through data analysis, public communication and engagement with vulnerable communities.
- Led by **Media Ecosystem Observatory** (McGill & U of T), in close collaboration with other academic and civil society organizations
- **$8M over 4 years** requested via B2022, through Canadian Heritage's proven Digital Citizen Initiative (co-chaired by PCO – Democratic Institutions); no new FTEs.
- **Support broader GoC engagement** with academia and civil society on democracy/technology nexus



Produce & support production of research on Canada's information ecosystem – e.g. patterns of info production, consumption and propagation – and impacts on attitudes and behaviours

Inform Canadians about the quality of information in the information ecosystem, including the identification of disinformation narratives and fact-checking

Government of Canada Gouvernement du Canada

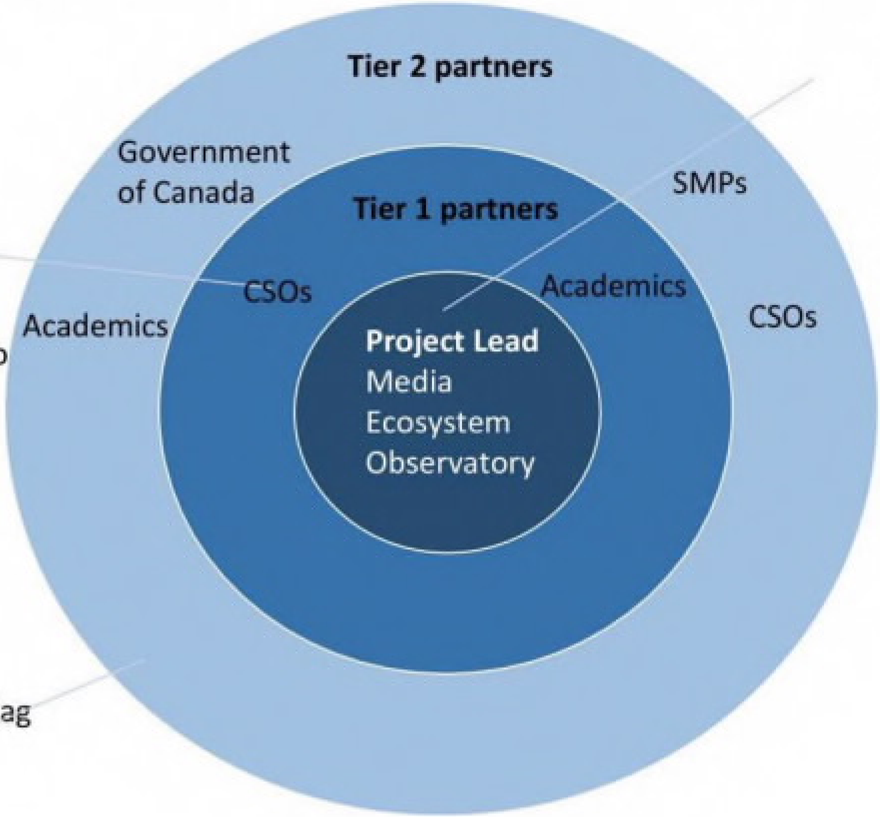
DRAFT

UNCLASSIFIED

The Online Integrity Network – stakeholder mapping

GoC defines project terms and scope through Contribution Agreement

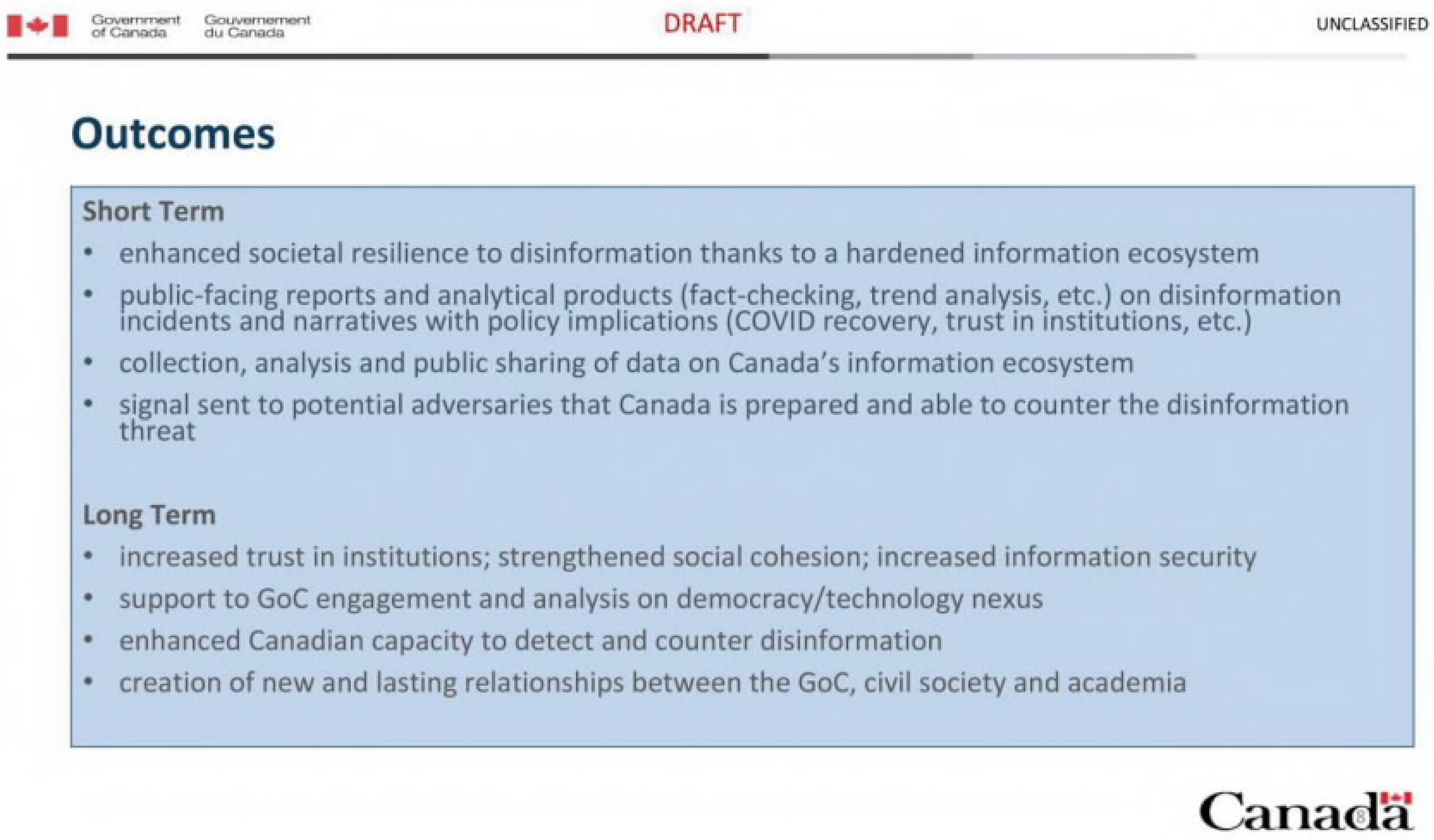
Tier 1 partners:
- ongoing analysis of info environment
- as-needed analysis of disinfo events
- public communication
- increased vigilance during periods of high disinfo risk (e.g. elections)



Project Lead:
- receives and manages funding
- interface with GoC
- coordinates research activities and public communications

Tier 2 partners:
- direct channel to Tier 1 to flag disinfo events

Canada



Government of Canada Gouvernement du Canada

DRAFT

UNCLASSIFIED

Outcomes

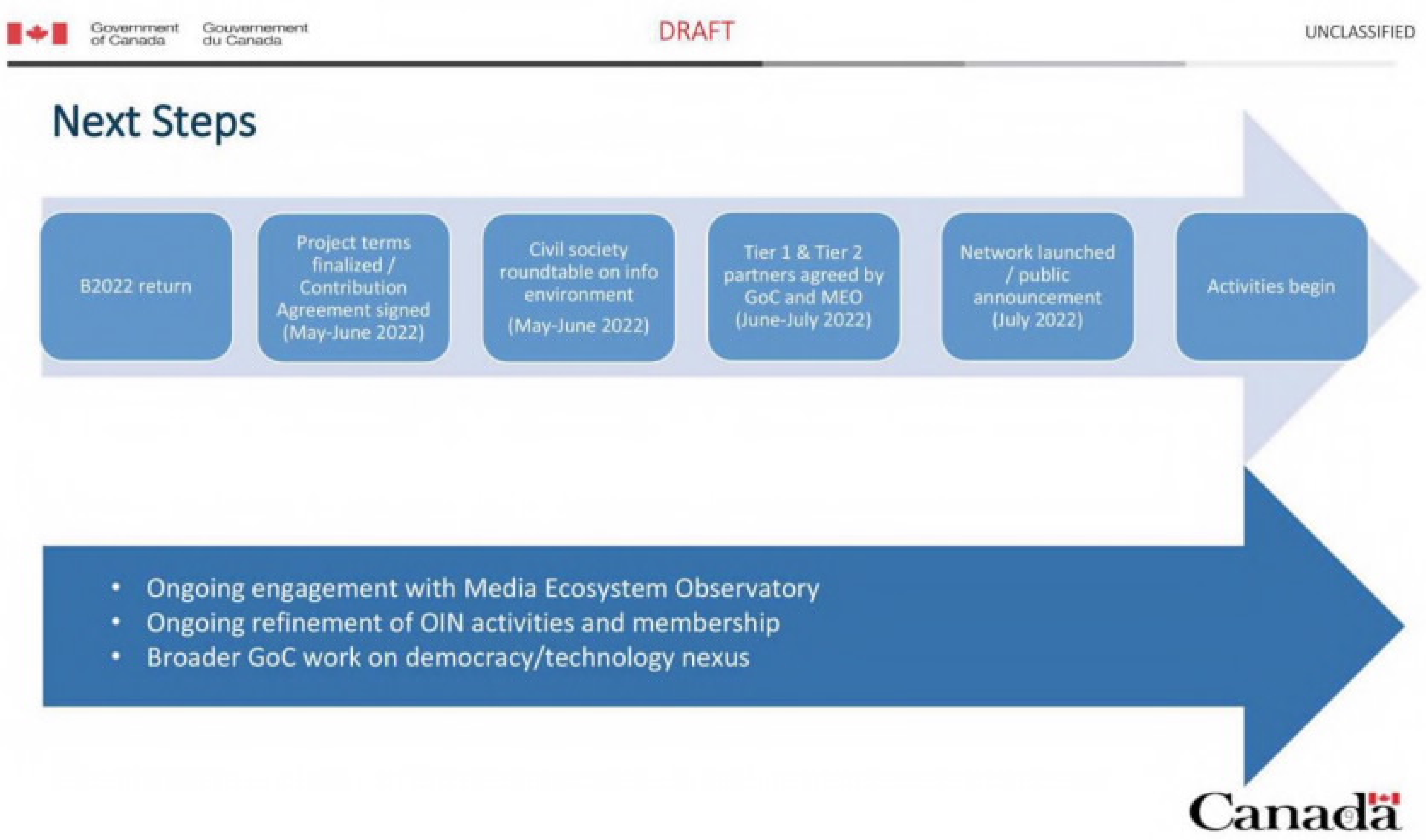
Short Term

- enhanced societal resilience to disinformation thanks to a hardened information ecosystem
- public-facing reports and analytical products (fact-checking, trend analysis, etc.) on disinformation incidents and narratives with policy implications (COVID recovery, trust in institutions, etc.)
- collection, analysis and public sharing of data on Canada's information ecosystem
- signal sent to potential adversaries that Canada is prepared and able to counter the disinformation threat

Long Term

- increased trust in institutions; strengthened social cohesion; increased information security
- support to GoC engagement and analysis on democracy/technology nexus
- enhanced Canadian capacity to detect and counter disinformation
- creation of new and lasting relationships between the GoC, civil society and academia

Canada



Government of Canada Gouvernement du Canada

DRAFT

UNCLASSIFIED

Next Steps

- B2022 return
- Project terms finalized / Contribution Agreement signed (May-June 2022)
- Civil society roundtable on info environment (May-June 2022)
- Tier 1 & Tier 2 partners agreed by GoC and MEO (June-July 2022)
- Network launched / public announcement (July 2022)
- Activities begin

- Ongoing engagement with Media Ecosystem Observatory
- Ongoing refinement of OIN activities and membership
- Broader GoC work on democracy/technology nexus

Canada

Slide Notes

Slide 1:
Brief introductory remarks:
grateful for opportunity to present
Canada learned from others in developing its Plan; we hope his will be useful to partners

3 parts of presentation:
Overview of PD 1.0
Successes/challenges of PD 1.0
Looking forward:
Brief overview of current threat picture (participant views welcome)
Next Steps for PD
Links to key documents provided on final slide

Slide 3:
Brief description of each tile – basic elements of threat assessment expected to be shared among participants.

Invite views of others on what has changed and what has stayed the same (for Q&A portion).

Slide 4:
Brief description of each tile – basic elements of threat assessment expected to be shared among participants.

Invite views of others on what has changed and what has stayed the same (for Q&A portion).

Slide 5:
PQPC tasked with reviewing PD 1.0 and developing recommendations. Much work done since 2019, and efforts nearing completion.

Assessments (both internal and independent) have revealed no fundamental flaws or major gaps in the Plan; therefore, we are looking to tweak and expand upon existing measures, as opposed to fundamentally rethinking our approach.

Cooperation and information exchange between governmental and nongovernmental actors are crucial to staying ahead of the game. [redacted] is a good example, as is the Paris Call for Trust and Security in Cyberspace.
Alongside Microsoft and the Aliance for Securing Democracy, Canada has co-led Principle 3 (« Defend Electoral Processes »); following a series of workshops that brought together experts and practitioners from governments, industry, academia and civil society, a compendium of best practices in countering election interference was released in April. Link on final slide
Since 2019, several other countries – including Australia, Denmark, New Zealand, UK, US – have made public plans to counter foreign interference, and we hope to learn from these experiences as well.

Canada's current situation is particular: while in principle we have fixed date elections (and can plan election-security measures accordingly), the 2019 election returned a minority government, meaning an election could theoretically occur at any time. We have therefore taken measures to ensure key activities can be implemented no matter when the next electoral campaign takes place.

Slide 6:
PQPC tasked with reviewing PD 1.0 and developing recommendations. Much work done since 2019, and efforts nearing completion.

Assessments (both internal and independent) have revealed no fundamental flaws or major gaps in the Plan; therefore, we are looking to tweak and expand upon existing measures, as opposed to fundamentally rethinking our approach.

Cooperation and information exchange between governmental and nongovernmental actors are crucial to staying ahead of the game. [redacted] is a good example, as is the Paris Call for Trust and Security in Cyberspace.
Alongside Microsoft and the Aliance for Securing Democracy, Canada has co-led Principle 3 (« Defend Electoral Processes »); following a series of workshops that brought together experts and practitioners from governments, industry, academia and civil society, a compendium of best practices in countering election interference was released in April. Link on final slide
Since 2019, several other countries – including Australia, Denmark, New Zealand, UK, US – have made public plans to counter foreign interference, and we hope to learn from these experiences as well.

Canada's current situation is particular: while in principle we have fixed date elections (and can plan election-security measures accordingly), the 2019 election returned a minority government, meaning an election could theoretically occur at any time. We have therefore taken measures to ensure key activities can be implemented no matter when the next electoral campaign takes place.

Slide 7:
PQPC tasked with reviewing PD 1.0 and developing recommendations. Much work done since 2019, and efforts nearing completion.

Assessments (both internal and independent) have revealed no fundamental flaws or major gaps in the Plan; therefore, we are looking to tweak and expand upon existing measures, as opposed to fundamentally rethinking our approach.

Cooperation and information exchange between governmental and nongovernmental actors are crucial to staying ahead of the game.
[redacted] is a good example, as is the Paris Call for Trust and Security in Cyberspace.
Alongside Microsoft and the Aliance for Securing Democracy, Canada has co-led Principle 3 (« Defend Electoral Processes »); following a series of workshops that brought together experts and practitioners from governments, industry, academia and civil society, a compendium of best practices in countering election interference was released in April. Link on final slide
Since 2019, several other countries – including Australia, Denmark, New Zealand, UK, US – have made public plans to counter foreign interference, and we hope to learn from these experiences as well.

Canada's current situation is particular: while in principle we have fixed date elections (and can plan election-security measures accordingly), the 2019 election returned a minority government, meaning an election could theoretically occur at any time. We have therefore taken measures to ensure key activities can be implemented no matter when the next electoral campaign takes place.

Slide 8:
PQPC tasked with reviewing PD 1.0 and developing recommendations. Much work done since 2019, and efforts nearing completion.

Assessments (both internal and independent) have revealed no fundamental flaws or major gaps in the Plan; therefore, we are looking to tweak and expand upon existing measures, as opposed to fundamentally rethinking our approach.

Cooperation and information exchange between governmental and nongovernmental actors are crucial to staying ahead of the game.
[redacted] is a good example, as is the Paris Call for Trust and Security in Cyberspace.
Alongside Microsoft and the Aliance for Securing Democracy, Canada has co-led Principle 3 (« Defend Electoral Processes »); following a series of workshops that brought together experts and practitioners from governments, industry, academia and civil society, a compendium of best practices in countering election interference was released in April. Link on final slide
Since 2019, several other countries – including Australia, Denmark, New Zealand, UK, US – have made public plans to counter foreign interference, and we hope to learn from these experiences as well.

Canada's current situation is particular: while in principle we have fixed date elections (and can plan election-security measures accordingly), the 2019 election returned a minority government, meaning an election could theoretically occur at any time. We have therefore taken measures to ensure key activities can be implemented no matter when the next electoral campaign takes place.

<u>Slide 9:</u>
PQPC tasked with reviewing PD 1.0 and developing recommendations. Much work done since 2019, and efforts nearing completion.

Assessments (both internal and independent) have revealed no fundamental flaws or major gaps in the Plan; therefore, we are looking to tweak and expand upon existing measures, as opposed to fundamentally rethinking our approach.

Cooperation and information exchange between governmental and nongovernmental actors are crucial to staying ahead of the game.
[redacted] is a good example, as is the Paris Call for Trust and Security in Cyberspace.
Alongside Microsoft and the Aliance for Securing Democracy, Canada has co-led Principle 3 (« Defend Electoral Processes »); following a series of workshops that brought together experts and practitioners from governments, industry, academia and civil society, a compendium of best practices in countering election interference was released in April. Link on final slide
Since 2019, several other countries – including Australia, Denmark, New Zealand, UK, US – have made public plans to counter foreign interference, and we hope to learn from these experiences as well.

Canada's current situation is particular: while in principle we have fixed date elections (and can plan election-security measures accordingly), the 2019 election returned a minority government, meaning an election could theoretically occur at any time. We have therefore taken measures to ensure key activities can be implemented no matter when the next electoral campaign takes place.