



Sécurité publique
Canada

Public Safety
Canada

BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**



Collaboration fédérale, provinciale et territoriale afin d'assurer la protection des Canadiens et des infrastructures essentielles du Canada contre les cybermenaces

Conseil des dirigeants principaux de l'information du secteur public (CDPISP)

Le 25 février 2016



- Le point sur les travaux de collaboration accomplis jusqu'à ce jour dans le cadre de la Stratégie de cybersécurité du Canada
- Une nouvelle approche en matière de cybersécurité à l'échelon fédéral
 - Examen cybernétique figurant dans la lettre de mandat du ministre
 - Plans à l'échelon fédéral pour assurer la protection des cybersystèmes essentiels
- Table ronde des sous-ministres fédéraux, provinciaux et territoriaux sur la cybersécurité
 - Composition de l'effectif
 - Plan d'action en matière de collaboration
- Prochaines étapes





Stratégie de cybersécurité du Canada

- Le cadre repose sur trois volets afin d'orienter les efforts du gouvernement du Canada :
 1. Assurer la protection des systèmes du gouvernement du Canada
 2. Nouer des partenariats pour assurer la protection des cybersystèmes essentiels à l'extérieur du gouvernement fédéral
 3. Aider les Canadiens à naviguer en ligne en toute sécurité
- Lancée en 2010, la Stratégie comprenait un investissement initial de 244\$ M; un autre investissement de 142,6\$ M a été annoncé en juillet 2015
- La plupart des investissements ont été réalisés dans le cadre du premier volet – étayé et sécurisé des réseaux et des systèmes gouvernementaux, engager maintenant le travail au-delà de la sphère fédérale
- Établissement de partenariats avec les provinces, les territoires et les secteurs des infrastructures essentielles
- Consolidation du Centre canadien de réponse aux incidents cybernétiques (CCRIC)
- Promotion de la sensibilisation, de l'éducation et de la mobilisation du public



Directives figurant dans la lettre de mandat du premier ministre



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

« Diriger un examen des mesures en place pour assurer la protection des Canadiens et des infrastructures essentielles contre les cybermenaces en collaboration avec le ministre de la Défense nationale, le ministre de l'Infrastructure et des Collectivités, le ministre des Services publics et de l'Approvisionnement, le ministre de l'Innovation, des Sciences et du Développement économique et le président du Conseil du Trésor. »

Objectifs de l'examen

- Mettre en place un processus crédible et complet de consultation des intervenants
- Cerner les besoins ainsi que les solutions et les innovations connexes
- Faire évoluer la cybersécurité du Canada vers le prochain niveau : passer d'une stratégie adaptée à une stratégie proactive, faire du Canada un chef de file mondial en matière de cybersécurité
- Élaborer un nouveau cadre national sur la cybersécurité



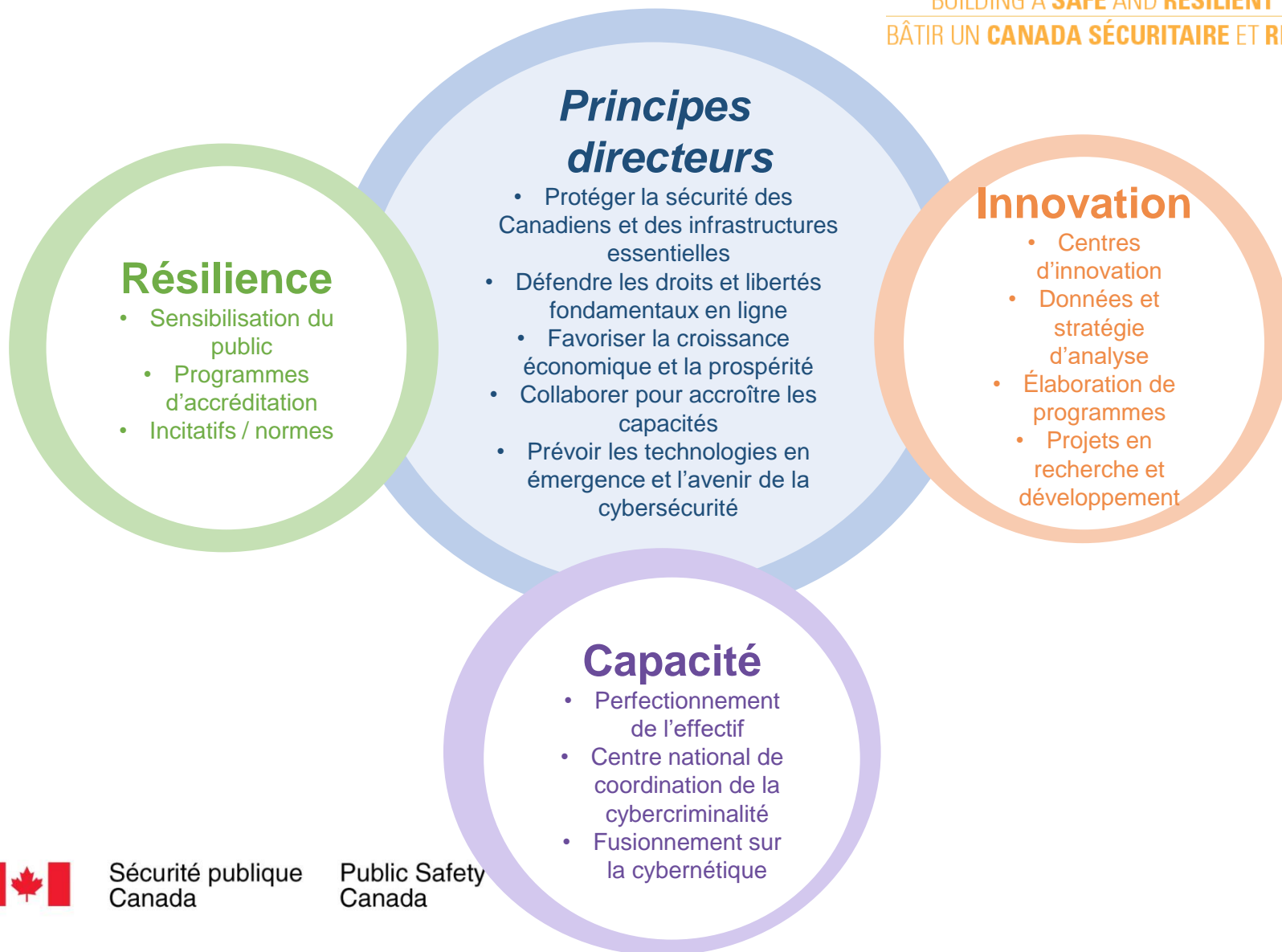
Sécurité publique
Canada

Public Safety
Canada

Cadre pour une approche renouvelée en matière de cybersécurité



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**



Sécurité publique
Canada

Public Safety
Canada

Processus d'examen



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

- Publier un document de consultation énumérant les principes et les principaux champs d'action (mars)
- Consulter l'industrie, les provinces et les territoires, les universités et la société civile (mars-juin)
- Recueillir les commentaires découlant de la consultation et élaborer un nouveau cadre, qui sera annoncé lors des premières initiatives au moyen d'un livre blanc (automne 2016)
- Offrir d'autres possibilités de mener des consultations et de formuler des commentaires sur des champs d'action après l'annonce du cadre
 - La question de la cybernétique ne propose pas une solution unique – il faudra faire évoluer les initiatives et les adapter



Processus de consultation



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

Consultations

- Solliciter des commentaires au moyen de divers mécanismes:
 - Possibilité pour les soumissions publiques - consultations en ligne
 - Ciblées tables rondes réunissant les fonctionnaires provinciaux et territoriaux
 - Utiliser véhicules d'engagement qui incluent la représentation FPT (groupes de travail, conseils, comités)

Solliciter les points de vue PT sur les éléments qui suivent

- Les défis urgents en matière de cybernétique dont il faut tenir compte pour promouvoir et protéger les infrastructures numériques du Canada
- Les lacunes qui subsistent pour assurer la protection des infrastructures essentielles du Canada et les Canadiens contre les cybermenaces
- L'établissement d'une base de référence des approches en matière de cybersécurité et de discuter de comment ces critères peuvent être adoptés à travers le Canada



Sécurité publique
Canada

Public Safety
Canada

Mesure préliminaire : Assurer la protection des cybersystèmes essentiels du Canada



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

- Parallèlement à l'examen, s'employer à prendre des mesures immédiates pour combler les lacunes
 - Élaborer des mesures législatives pour assurer la protection des cybersystèmes essentiels conformément aux annonces figurant dans le Budget de 2015
- Lacune actuelle: aucun mécanisme n'est en place de sorte que les cybersystèmes maintiennent un niveau de sécurité élémentaire malgré les risques pour la sécurité nationale, la sécurité publique et l'économie du Canada
 - Cette lacune nuit à la capacité du gouvernement d'aider les exploitants de cybersystèmes essentiels
- Il faut adopter une approche de collaboration entre les exploitants du secteur privé et le gouvernement:
 - renforcer la défense collective au profit de la sécurité nationale et de l'économie du Canada
 - jeter le fondement de l'échange de renseignements et de l'expertise



Sécurité publique
Canada

Public Safety
Canada

Assurer la protection des cybersystèmes essentiels du Canada



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

Contexte

- Aucun fondement juridique ne permet de détecter ou de protéger les cybersystèmes essentiels
- La capacité d'aider les exploitants, de préserver l'économie et de protéger la sécurité nationale est limitée
- De nombreux pays examinent des approches législatives
- Budget de 2015: des mesures législatives ont été annoncées pour assurer la protection des cybersystèmes essentiels



Sécurité publique
Canada

Public Safety
Canada



IDENTIFICATION

- Désignation des cybersystèmes essentiels et de leurs propriétaires

PROTECTION

- Plans de cybersécurité
- Signalement des incidents
- Directives en cas d'urgence
- Sanctions pénales en cas d'attaques contre les systèmes essentiels

COLLABORATION

- Soutien lors de crises
- Expertise et outils
- Renseignement permettant un suivi
- Analyse en temps réel et à long terme



Table ronde des sous-ministres fédéraux, provinciaux et territoriaux sur la cybersécurité



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

Contexte

- La Table ronde a été organisée par suite d'une réunion du greffier et des secrétaires de Cabinet qui a eu lieu en juillet 2013
- Deux réunions sont tenues annuellement; la plus récente a été organisée le 10 juin 2015
- La Table ronde offre une tribune permettant d'échanger des renseignements et des pratiques exemplaires sur le renforcement de la cybersécurité, de définir des termes propres à la cybersécurité, de donner une orientation stratégique et de déterminer les principales activités et réalisations attendues des gouvernements FPT

Difficultés

- Les administrations possèdent des capacités distinctes et divers niveaux de maturité en ce qui a trait à la cybersécurité
- Les administrations ont des approches différentes face à la cybersécurité – priorité relative à la sécurité des TI, aux infrastructures ou à la sécurité publique
- La cybersécurité est à la fois complexe et dynamique; elle requiert une analyse globale et une stratégie d'engagement à multiples facettes



Sécurité publique
Canada

Public Safety
Canada

Plan d'action de collaboration



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

Quatre secteurs d'activités convenus qui nécessitent la collaboration FPT :

1. échange de renseignements et intervention en cas d'incident (sous la direction de Sécurité publique Canada [SP])
2. sensibilisation du public (responsables : Colombie-Britannique et SP)
3. normes et pratiques exemplaires en matière de cybersécurité (responsables: Alberta, Ontario et SP)
4. formation et gestion des talents (responsables: Nouveau-Brunswick et SP)

Les révisions proposées par la DGCN et approuvées par SCDPI au cours de l'automne 2015:

- deux activités ont été transférées au SCDPI
- entente sur les priorités qui s'inscrivent dans le Plan d'action; Cependant, les ressources limitées sont un problème
- nécessité de designer des responsables dans des domaines d'expertise outre la sécurité des TI



Sécurité publique
Canada

Public Safety
Canada

Les prochaines étapes



BUILDING A **SAFE AND RESILIENT CANADA**
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

Éléments du plan d'action

- Selon vous, quelle personne au sein de votre province ou territoire (représentant principal et un remplaçant) serait bien placée pour faire partie de la Table ronde des sous-ministres fédéraux, provinciaux et territoriaux sur la cybersécurité ?
- Comment pouvons-nous faire avancer les priorités figurant dans le Plan d'action?

Processus d'examen

- Quels sont les défis urgents en matière de cybernétique auxquels le gouvernement devrait s'attaquer afin de promouvoir et de protéger les infrastructures numériques du Canada?
- Selon vous, quelles sont les lacunes sur le plan des politiques et des opérations qui persistent en matière de protection des infrastructures essentielles du Canada contre les cybermenaces?
- Comment pouvons-nous favoriser une approche législative pour assurer la protection des cybersystèmes essentiels et mobiliser davantage le secteur privé en vue d'établir des normes?
- Comment faire du Canada un chef de file mondial de la cybersécurité et veiller à ce que la cybersécurité soit l'un de ses atouts concurrentiels ?



Sécurité publique
Canada

Public Safety
Canada



Direction générale de la cybersécurité nationale, Sécurité publique Canada :

Mark Matz, directeur, Politiques et gestion des enjeux

mark.matz@canada.ca

