NON-CLASSIFIÉ

Service canadien du renseignement de sécurité

Canadian Security Intelligence Service

LES VILLES INTELLIGENTES ET LA SÉCURITÉ NATIONALE

DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.
A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.

Canada

/// QU'ENTEND-ON PAR VILLE INTELLIGENTE?

On trouve de nombreuses définitions de *ville intelligente*. Dans le présent document, une ville intelligente s'entend d'un milieu urbain dans lequel des technologies numériques sont utilisées pour améliorer la qualité et l'efficacité des services municipaux. Dans une ville intelligente, on recueille des données sur l'utilisation des infrastructures publiques et les interactions avec les utilisateurs, puis on les analyse en vue d'améliorer la prestation des services et l'expérience de la population. Ces données sont recueillies à l'aide de capteurs et de dispositifs intégrés à un réseau centralisé qui gère la prestation de services.

Le concept de ville intelligente peut être adapté aux besoins et aux intentions de la collectivité. Au nombre des principaux facteurs qui contribuent à l'« intelligence », mentionnons la quantité et la qualité des données recueillies, le degré d'interaction des différents réseaux d'infrastructures et la manière dont les propriétaires et les exploitants des infrastructures utilisent les données pour prendre des décisions éclairées.

/// VILLES INTELLIGENTES AU CANADA

On ignore le nombre officiel de projets de ville intelligente en cours au Canada, mais les projets de la sorte suscitent manifestement beaucoup d'intérêt. Dès 2017, lorsque le gouvernement du Canada a lancé le Défi des villes intelligentes, plus de 225 municipalités — petites villes, communautés autochtones et grands centres urbains de toutes les provinces et de tous les territoires — qui souhaitaient explorer les avantages des villes intelligentes ont posé leur candidature.

/// TYPE DE DONNÉES RECUEILLIES ET MÉTHODES DE COLLECTE

Pour avoir une idée du type d'informations qui peuvent être recueillies au sein d'une ville intelligente, il suffit de penser aux applications possibles : services publics intelligents, maisons intelligentes, véhicules autonomes, hôpitaux intelligents, commerces intelligents et transport en commun intelligent.

À titre d'exemple, des technologies de gestion de la circulation ou du transport pourraient recueillir des données qui donnent une image des mouvements des personnes dans la ville ainsi que d'autres données connexes. Ces renseignements personnels pourraient être recueillis par des capteurs, tels que des dispositifs d'enregistrement audio et vidéo ou des lecteurs de plaques d'immatriculation, ou des appareils mobiles personnels.

/// PRÉOCCUPATIONS EN MATIÈRE DE SÉCURITÉ NATIONALE

Les villes intelligentes représentent la prochaine génération d'infrastructures essentielles à la base de pratiquement tous les aspects de la vie. En raison de cette centralisation, les villes intelligentes constitueront des cibles de choix pour les activités d'espionnage, de sabotage et de perturbation des criminels et des acteurs étatiques hostiles.

Exploitation des données :

Les villes intelligentes recueilleront et traiteront d'énormes quantités de données personnelles et organisationnelles produites par l'utilisation des infrastructures intelligentes et les interactions avec les utilisateurs. Ces données peuvent fournir aux auteurs de menaces de précieuses informations, notamment sur les profils et les habitudes de vie de Canadiens. Un auteur de menace peut exploiter de telles données pour mener des activités (espionnage, ingérence étrangère, etc.) qui compromettent la sécurité de la population canadienne et des infrastructures essentielles du Canada.

Interconnexion des infrastructures essentielles :

La connexion des différentes infrastructures essentielles à des réseaux de télécommunication augmente la « superficie d'attaque » ainsi que l'ampleur potentielle des conséquences d'une attaque. Ainsi, l'accès à une infrastructure essentielle ou la perturbation d'une telle infrastructure pourrait avoir des répercussions sur d'autres systèmes.

/// CONSÉQUENCES NÉFASTES D'UN ACCÈS NON AUTORISÉ OU D'UNE GOUVERNANCE INADÉQUATE DES DONNÉES

- La perturbation des infrastructures ou des services publics (p. ex. le transport en commun, le contrôle de la circulation, la répartition des appels d'urgence et l'approvisionnement en eau ou en électricité) ou le déni d'accès à ces infrastructures.
- L'accès non autorisé à des données personnelles ou organisationnelles, leur conservation ou leur exploitation peut faciliter les activités d'espionnage et d'ingérence étrangère contre des individus ou des groupes. Voici quelques exemples :
    - La collecte et l'usage impropre de renseignements personnels ou d'images prises par des caméras de surveillance.
    - La perturbation de systèmes et le vol ou la corruption de données.
    - L'espionnage de collectivités ciblées et les menaces subséquentes (harcèlement ou intimidation) contre des membres de ces collectivités.
- L'utilisation de grandes quantités de données canadiennes à l'appui de la recherche menée par des États étrangers pour mettre au point des systèmes militaires ou des programmes de surveillance de pointe (p. ex. améliorer des algorithmes d'intelligence artificielle utilisés pour des capacités avancées sur le plan militaire ou du renseignement).

/// COMMENT LES VILLES INTELLIGENTES PEUVENT-ELLES ÊTRE COMPROMISES?

Méthodes possibles :

- Cyberattaques
- Menace interne
- Compromission de l'équipement ou des chaînes d'approvisionnement
- Accès aux systèmes (ou à leurs données) par des acteurs de l'extérieur au moment de l'installation, de l'opération, de l'entretien ou de la maintenance de ces systèmes

/// PRINCIPAUX FACTEURS À CONSIDÉRER AVANT D'ADOPTER LE CONCEPT DE VILLE INTELLIGENTE

- Intégrer la gouvernance et la sécurité des données à toutes les phases du cycle de vie d'un projet de ville intelligente, de la conception à la mise hors service.
- Trouver les pratiques exemplaires à l'échelle internationale et les appliquer pour assurer la sécurité des terminaux et des appareils, des réseaux, des données et des applications.
- Sensibiliser les citoyens dès le début du projet pour qu'ils connaissent et comprennent les implications sur le plan de la protection des renseignements personnels et de la sécurité, et faciliter la tenue de véritables consultations publiques.
- Faire preuve de transparence envers les citoyens relativement aux données recueillies, à leur utilisation, à l'endroit où elles sont conservées et à la façon dont elles sont protégées.
- Faire preuve de diligence raisonnable. Évaluer avec soin les technologies pour les villes intelligentes, les fournisseurs de logiciels et leur chaîne d'approvisionnement pour s'assurer que l'accès aux données ainsi que le stockage, le transfert et l'utilisation des données s'effectuent d'une manière et à un endroit qui garantissent la sûreté, la sécurité et la protection de la vie privée de la population canadienne.
- Étudier attentivement toutes les dispositions relatives à l'accès, à la gouvernance et au stockage des données et demander un avis juridique ou des conseils en matière de sécurité avant de signer un contrat avec un fournisseur.
- S'assurer que le contrat avec le fournisseur comprend des dispositions claires et exécutoires en matière de règlement des différends.
- Effectuer des évaluations des risques relatifs aux renseignements personnels et à la sécurité avant de déployer des applications ou des plateformes de ville intelligente.
- Élaborer des plans d'intervention rapide en cas d'incident critique (p. ex. atteinte à la sécurité des données ou cyberattaque) et s'exercer à les mettre à exécution.

NOTES

NOTES

CONTACTEZ-NOUS

Canada.ca

Renseignements généraux : 613-993-9620

Signaler des informations relatives à la sécurité nationale : 1-800-267-7685

ISBN : 978-0-660-39470-1
N° de cat. : PS74-15/2021F-PDF
Also available in English under the title: *Smart cities and national security*