



[Canada.ca](#) › [Canadian Security Intelligence Service](#) › [Publications](#) › [smart-cities-national-security](#)

Smart Cities and National Security

On this page

- [What are smart cities?](#)
- [Smart Cities in Canada](#)
- [What kind of data is collected, and how?](#)
- [What are the national security concerns?](#)
- [Possible harmful impacts of a smart city city breach or inadequate data governance](#)
- [How can smart cities be compromised?](#)
- [Key considerations for smart city adoption](#)

What are smart cities?

There are many definitions of a 'smart city.' Here, we refer to environments where digital technologies are used to enhance the quality and efficiency of municipal services. A 'smart' city collects and analyses data interactions with, and usage of, public infrastructure in order to improve service delivery and user experience. This data is collected through connected sensors and individual devices which are part of centralized networks that manage service delivery.

Smart cities can be scalable according to the needs and intentions of the community. Key factors that shape 'smartness' include the quantity and quality of data collected, the degree of interaction of different infrastructure networks, and how the data is used to inform decisions by infrastructure owners and operators.



[Smart Cities and National Security](#)
[PDF (Portable Document Format) - 10.35 MB (Megabyte)]

Smart Cities in Canada

There is no definitive tracking on the number of smart city projects currently underway in Canada, but there is clearly a high level of interest. As early as 2017, when the Government of Canada Smart Cities Challenge was launched, over 225 municipalities expressed interest in exploring smart city benefits by submitting applications. Municipalities from every province and territory, including small towns, Indigenous communities and large urban centres all applied.

What kind of data is collected, and how?

To give you a sense of the kind of information that could be collected in a smart city, consider these smart city applications: smart utilities, smart homes, autonomous vehicles, smart hospitals, smart commerce and smart public transportation. To provide one example, smart city technologies used to manage traffic or transportation might collect data that provide a picture of individuals' movements in a city, and other related data. This personal information could be collected from sensors, such as audio and video recording devices or vehicle licence plate readers, or from personal mobile devices.

What are the national security concerns?

Smart cities represent the next generation of critical infrastructure, underpinning nearly all aspects of daily life. This integrated centrality means that smart cities will be attractive targets of hostile state actors and criminals for espionage and sabotage/disruption.

Data exploitation:

Smart cities will collect and operate by processing huge volumes of personal and corporate data produced through interactions with, and usage of, smart infrastructure. This data can provide valuable insights for threat actors, including profiles and patterns of life of Canadians. In the hands of a threat actor, this data can be exploited to enable activities that compromise the safety and security of Canadians (e.g. espionage, foreign interference) and Canadian critical infrastructure.

Interconnected Critical Infrastructure:

Connecting different critical infrastructure systems via telecommunications networks increases both the 'attack surface' and the potential scale of impact (i.e. access to or disruption of one infrastructure systems could have spillover effects on other systems).

Possible harmful impacts of a smart city city breach or inadequate data governance

- Disruption or denial of access to public infrastructure or services such as public transit, traffic control, emergency dispatch or utilities (e.g. water or electricity).
- Unauthorized access to, retention of, or exploitation of, Canadians' personal and corporate data, which could be used to facilitate further targeting of individuals and communities for foreign interference or espionage. Examples of such activities would include:
 - Capture and misuse of personal information or surveillance footage.
 - Disruption, theft, or corruption of Canadian data, information and systems.
 - Espionage against targeted communities, and subsequent threat activities against members of the community such as harassment or intimidation.
- Use of large amounts of Canadian data to support research for the benefit of foreign states in developing advanced military systems and or surveillance programs (e.g. Canadian data used to train AI algorithms of advanced military or intelligence capabilities).

How can smart cities be compromised?

Methods can include:

- Cyber Operations
- Insider Threat
- Compromised Equipment or Supply Chains
- External Actor Access to Systems or Data during Installation, Maintenance, Operation or Servicing

Key considerations for smart city adoption

- Integrate data governance and security into all phases of a smart city project, from design, throughout operation, to decommissioning.
- Identify and apply global best-practices to ensure security of endpoints and devices, networks, data, and applications.
- Engage citizens early to ensure awareness and understanding of the privacy and security implications to facilitate meaningful public consultation.
- Be transparent with citizens about the data collected in smart cities and the ways it is used and handled, where it is stored, and how it is protected.

- Do your due diligence. Smart city technology and software vendors, and their supply chains, should be assessed very carefully to ensure that data access, storage, transfer, and use will take place in a manner and location that protects the safety, security and privacy of Canadians.
- Review all data governance, access, and storage provisions carefully, and seek legal and security guidance before concluding a vendor agreement.
- Ensure that vendor agreements include clear and enforceable dispute resolution provisions.
- Conduct privacy and security risk assessments before deploying any smart city applications or platforms.
- Prepare for and practice critical incident response to ensure a rapid response in case of incidents (e.g. data breach, cyber attack).

Date modified:

2022-02-16