Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

Smart Cities: Challenges and Opportunities for Public Safety and Security

Helen Tang
Paul Hubbard
Suzanne Waldman

DRDC – Centre for Security Science

Defence Research and Development Canada
Scientific Letter
DRDC-RDDC-2018-L002
January 2018

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Endorsement statement: This publication has been peer-reviewed and published by the Editorial Office of Defence Research and Development Canada, an agency of the Department of National Defence of Canada. Inquiries can be sent to: Publications.DRDC-RDDC@drdc-rddc.gc.ca.

Defence Research and Development Canada | Recherche et développement pour la défense Canada

DRDC | RDDC
technologysciencetechnologie

January 2018

DRDC-RDDC-2018-L002

Prepared for: Mark Williamson, A/ADM S&T

Scientific Letter

Smart Cities: Challenges and Opportunities for Public Safety and Security

Purpose

In May of 2017, the Director General of Defence Research and Development Canada's Centre for Security Science (DRDC CSS), currently the Acting Assistant Deputy Minister of Science and Technology (ADM S&T) at Department of National Defence, requested an overview of the range of challenges and opportunities for public safety and security presented by the Smart Cities paradigm of innovation to inform CSSP strategic planning. This scientific letter presents a response to this request by reporting on how smart cities technologies can enhance public safety, security, and resilience; to detail the security and privacy issues simultaneously raised by the smart cities paradigm; and to offer recommendations for how the CSSP can navigate this domain.

Background

The smart cities paradigm, which leverages the Internet of Things (IoT) to enhance the capabilities of city managers to monitor and respond to city conditions of all kinds in real time, is currently in the foreground in municipal planning and technology development internationally. Smart cities can be seen as wide-scale cyber-physical systems in which sensors monitor cyber and physical indicators, prompting actuators to make dynamic changes in the complex urban environment. Both United States and Canada have launched smart cities challenges to inspire innovation in this domain, and an International Pavilion to exhibit smart cities capabilities was meanwhile recently held in Montreal (October 2017). In the domain of public safety and security, the smart cities paradigm holds both potential for enhancing community safety, security, and resilience in the coming era, while also opening up novel security issues and challenges to be addressed.

Smart cities are conceptualized as complex, networked Internet of Thing (IoT) devices and communications infrastructure for handling different services and systems throughout the cities and optimizing resource consumption. The smart city concept refers to applying all available technology and resources in a coordinated manner [1]; see Table 1 for an overview of smart city elements.

Canada

Table 1: Smart city elements.

Smart transportation will enable efficient, coordinated mobility through the use of technologies and solutions, such as low emission cars and multimodal transport systems; *Smart buildings* will use advanced automated infrastructure to control and manage multiple aspects such as lighting and temperature, security, and energy consumption independently or with minimal human intervention; *Smart technology* will connect features of an individual's home, office space, mobile phone, and car on a single wireless platform; *Smart healthcare* will use remote communications systems, such as eHealth and mHealth with connected medical devices to enhance health monitoring and diagnostics; *Smart infrastructure* will be automated systems that manage energy grids, transportation networks, water and waste management systems to improve efficiency, monitoring, and dynamic adaptations to changing conditions; *Smart energy* will incorporate advanced meter infrastructure (AMI) and distribution grid management to accelerate demand response amid the integrated transmission and distribution of power; *Smart security* will combine video surveillance and next generation policing uniforms equipped with built in sensors and network connections to enable data analytics to protect people, property, and information; *Smart governance* and *smart education* will support the adoption of smart city technologies through policies, services, incentives, subsidies, or other promotions; [2][3]

As 54% of the world's population currently lives in urban areas, it will require huge investments to upgrade old-economy cities and fulfill the vision of the smart city, with the smart cities market expected to be worth $1.2 trillion (USD) by 2022 [4]. This massive retrofitting will involve hundreds of thousands of sensors becoming deployed throughout cities, feeding big data urban management system and commercial applications that stream real-time information to city managers, workers, and residents.

While much prospective smart cities technology is not yet mature, over the short term the introduction of smart capabilities can be approached incrementally by adding sensors and actuators opportunistically as innovations occur in application. Ultimately, increasingly sophisticated machine learning applications will be available to coordinate information derived from sensors, video cameras, and other inputs, providing analytical filters to monitor conditions and identify events and requirements amid what would otherwise be information overload [5]. Additional research and development will meanwhile be required over coming decades to ensure that the security and privacy of smart cities' informational and infrastructural elements are protected from malicious actors. Effort is also required to build structures that allow citizens to submit not merely their data but also their observations, ideas, and values to the governance of communities [5][6].

Opportunities for Community Safety, Security, Resilience

On a day-to-day basis, smart community technologies are expected to make cities safer, more comfortable, and more efficient places for people to live. Smart technologies such as sensors, mobile and network technology, big data analytics, and artificial intelligence applications are expected to bolster community resilience by facilitating "a diverse and decentralized collection of structures that back up each service within every infrastructure system" ensuring services are continuously well-managed [7][8]. Smart social technologies prospectively include more agile real-time social media networking, alerting, information access, and recruitment; and the creation of more extensive and open government input and accountability channels.

Specific areas of opportunity for expanding community safety, security, and resilience include:

Sensor and monitoring technology: IOT enabled sensors will be able to support a wide variety of safety and security functions. Traffic sensors will detect vehicle accidents and conditions while triggering traffic signals to ensure the right of way for first responders. Monitoring techniques will enable more frequent and accurate assessment of road quality and target interventions before problems become major failures. New enhanced video monitoring platforms will provide deep learning analytics to video streams produced from the nearly 1 billion cameras worldwide foreseen to be in operation by 2020 in government properties, public transit systems, commercial buildings, and roadways [9]; see Table 2 for current applications of smart sensor and monitoring technology.

Table 2: Smart sensor and monitoring technology.

HAAS (Heedful Audio Alert System) in Chicago uses V2V (vehicle-to-vehicle) communication to alert drivers to approaching emergency vehicles in real time, with push notifications to drivers and cyclists. The program is hoped to enhance live fleet management and response rate data analysis to save lives as well as millions of dollars in emergency vehicle collision repairs and lawsuits [10].
AI-enhanced video surveillance technology can already monitor surveillance camera videos in real time for smoke detection, fire detection, and unattended baggage [11].
A sound-based sensor network embedded in GE intelligent street lights that identifies gunfire alerted law enforcement to 74,916 gunfire incidents in 2016 [7].

Smart infrastructure: Sensors on buildings or other infrastructure (such as streetlights) will monitor for energy outages and excessive heat, pollution, radiation, vibration, and flood conditions. Smart flood defences and networked communications and electrical grids with built in redundancy and fast recovery capabilities will respond and reroute in the face of stresses [12].

Table 3: Smart infrastructure technology

Seattle currently runs a "RainWatch" application that combines radar data with a network of rainfall gauges, allowing city maintenance workers to respond quickly to flooding incidents and to issue alerts to residents [7].

Policing applications: Policing capabilities stand to improve through smart technologies. Automated license plate readers will help track incidents such as hit-and-runs. Gunshot detectors will detect crimes in process, while CCTV security cameras enabled with artificial intelligence could provide additional alerts and information. Body-worn video monitors can contribute data for real-time and retrospective crime analysis. Sensors worn by police can keep them situationally aware and connected to real-time information feeds about evolving incidents. Policing analysis can become increasingly real-time, identifying ongoing or potential criminal acts by combining and analyzing data from a variety of sources, including CCTV and social media platforms such as Twitter to monitor and prevent crime. Predictive capabilities can be enhanced by running data through machine learning applications that monitor for patterns, catch trends, extract key insights, and identify crime hot spots; see Table 4 for applications of smart policing technology.

Table 4: Smart policing technology.

AUDREY, the Assistant for Understanding Data through Reasoning, Extraction, and sYnthesis, was developed by Pasadena, California NASA Jet Propulsion Laboratory (JPL), to keep firefighters, police, paramedics and other first responders safe in the field **by** tracking teams of first responders and making recommendations to individual operators on how to best coordinate [13]**.**
In 2014, Stockton, CA launched a program of analyzing data on non-domestic gun violence-related crimes to identify trends and flag forecast zones where incidents are likely to occur. The police department began deploying resources to these zones in increasing numbers, and preliminary numbers for March through May 2016 showed 40 to 60 percent month-to-month decreases in non-domestic gun violence-related crimes in forecast zones [14].

Social technologies: Smart social technologies permitted by expanded network communications include greater open government and open data opportunities for citizens to remain apprised of and supply input into municipal business and decisions [15]. The Toronto Region Board of Trade defines a smart city as "an urban region that uses information and communication technologies (ICT) and digital connectivity to enhance the quality and performance of city services, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens"[5]. Social technologies include more spontaneous engagement of city managers with citizens via social media channels to keep them apprised of conditions and to obtain information, support, and voluntary participation in the face of requirements. Social media will be an important channel of citizen information on ongoing incidents through Public Safety Broadband-enabled applications such as Next Generation 911. Meanwhile, social media monitoring enhanced by artificial intelligence is becoming an important source of real-time situational awareness of ongoing incidents and stands to become an increasingly acute source of day-to-day information for first responders as artificial intelligence plays a stronger role.

Table 5: Smart social technology.

Increasingly, citizens can be informed regarding locational risks and conditions through content pushed by beacons to proximate smartphones [16]**.**
Cities around the world are using online tools to enable Participatory Budgeting programs where citizens submit ideas and vote on budgetary expenditures. [16]
In the 2013 flood, the City of Calgary used Twitter to recruit citizens to help with emergency volunteering tasks [17].

Smart public services using blockchain: In cities, governments are responsible for governance, the economy, social issues, mobility, security, culture and the environment. These activities consist of a myriad of different processes that require a high frequency of registration and documentation and where transparency and security are essential, such as in the creation of contracts and permits. Blockchain may offer a technology to add legitimacy and privacy to these processes, as one of its main characteristics is a neutral, non-hierarchical, accessible and secure information database.

Table 6: Smart public services using blockchain.

Dubai provides an example of how using blockchain in transactions can enable smart city technologies. The following proofs of concept have been unveiled: [18] * Digitize health records on blockchain to provide patients and care providers with secure access to medical data; * Digitize and transfer Kimberley certificates on blockchain to secure the diamond trade. * Transfer titles of illiquid assets on blockchain to increase trade efficiency; * Streamline ID verification to reduce business registration times; * Use blockchain-based wills and contracts to ease transfer of ownership; * Boost tourism in Dubai through a blockchain-based program that would allow visitors to earn and spend loyalty points; * Apply blockchain to trade finance to more effectively exchange goods and the financing for those goods.

Smart cities security and privacy issues and challenges

Diverse data security, privacy, and protection issues and challenges will inevitably be raised by smart cities applications such as those described above, insofar as they involve generating, processing, analyzing, sharing, and storing large amounts of actionable data [19] [20] [21] [22]. These issues and challenges will pertain to:

IoT Devices Security and Privacy: IoT devices play an important role among the diverse layers of smart cities for collecting, transferring, temporary storing, and analyzing data. There are numerous special security and privacy issues challenges raised by these devices due to their heterogeneity, low computational resources, and lack of regulatory standards bearing on them. One factor that may help in securing these technologies could be the creation of efficient, secured, and lightweight cryptographic algorithms, such as those used by blockchain, that can provide secure end-to-end communication channels [23].

*Data privacy and protection***:** In general terms, privacy debates concern acceptable practices with regards to accessing and disclosing personal and sensitive information about persons. Smart city capabilities for monitoring massive amounts of data will greatly expand the volume, range and granularity of the data being generated about people and places and, in turn, will raise significant privacy issues.

In particular, smart cities are likely to raise risks of data capture malpractices including: identity-based surveillance; data aggregation involving the combining of data about persons to identify trends or patterns of activity; data leakage, or improper access to sensitive information permitted by inadequate data protection policies; and extended usage, or the collection of data for periods longer than expressly permitted or for purposes other than that to which the subject has consented [24]. Privacy concerns will further be opened up in smart cities due to the ubiquitous use of smartphones, which will be key technologies through which citizens interface with and experience the smart city.

Insecure components: Collecting data in smart cities will depend on deploying a large number of sensors, many of which may be insecure and not thoroughly tested. Sensor technology is especially susceptible to hacking due to its lack of standardization, potentially permitting pernicious individuals to introduce fake data that can cause signal failures and system shutdowns [25].

*Enlarged attack surface***:** Smart city operations will employ complex, networked communications infrastructure to effectively manage numerous services. With most of this infrastructure connected to the network, the number of potential entry points by which malicious actors could penetrate the system as a whole will be multiplied. Employees gaining access to municipal or other networks to access work-related data through their personal devices could additionally elevate security risks to the smart city through vulnerabilities such as malware, malicious codes, security holes, and security weaknesses that could allow unauthorized persons to enter the system and access classified information [21].

*Bandwidth exhaustion***:** The large number of sensors or actuators a smart city will put in communication could create a floods of data traffic sufficient to bring down servers. The bandwidth consumption from billions of devices could put a strain on the entire spectrum of wireless communications operating on megahertz frequencies, including radio, television, and emergency services [26].

Recommendations:

DRDC CSS is in a unique position to provide S&T advice regarding smart cities implementation and security, which is a cross-departmental issue. The following S&T challenges are recommended for future CSSP strategic planning guidance:

1) Applications of Smart Cities Technologies to Community Safety, Security, and Resilience

Innovation is required to develop applications for the Canadian context that enhance urban and rural safety, security, and resilience in fields such as policing and intelligence; emergency prevention and management; infrastructure system monitoring and protection; fire protection and response; community paramedicine; and first responder rural hub technology. Such applications will increasingly require the incorporation of machine learning/artificial intelligence elements permitting them to monitor, filter, analyze, integrate, and communicate massive amounts of IoT information. Further, social technologies allowing citizen values to be reflected in meaningful and accountable ways in governance, including open government and social media engagement strategies, will be needed to augment the data-focus of smart communities to ensure the levels of ongoing civic engagement required for resilient communities.

2) Security and Privacy by Design

Innovation is required to make Smart Cities more robust to cyber-attacks and privacy invasions by anticipating specific vulnerabilities, threats and opportunities that the paradigm poses and improving the security posture of large integrated cyber-physical systems overall. The most effective security and privacy innovations are likely to be introduced at the system-design level, ensuring they are comprehensive rather than piecemeal and well-matched to specific challenges posed by evolving cyber-physical landscapes.

Prepared by: Helen Tang, Paul Hubbard, and Suzanne Waldman (DRDC – Centre for Security Science).

References

[1] J. M. Barrionuevo, P. Berrone, & J. E. Ricart, "Smart Cities, Sustainable Progress," vol. 14, no. pp. 50–57, 2012.

[2] C. Benevolo, R. P. Dameri, and B. D'Auria, "Smart Mobility in Smart City," in *Empowering Organizations: Enabling Platforms and Artefacts*, Cham, Springer International Publishing, pp. 13–28, 2016.

[3] H. Chourabi et al., ""Understanding Smart Cities: An Integrative Framework," in 45th International Conference on System Sciences, Hawaii, 2012.

[4] Marketsandmarkets.com, "Smart Cities Market: Global Forecast to 2022," July 2017. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html. [Accessed 1 October 2017].

[5] G. Plunkett, "What is a smart community?," ESRI, 12 December 2016. [Online]. Available: https://resources.esri.ca/spatial-data-infrastructure/what-is-a-smart-community. [Accessed 1 October 2017].

[6] J. Walker, "Smart City Artificial Intelligence Applications and Trends," 8 August 2017. [Online]. Available: https://www.techemergence.com/smart-city-artificial-intelligence-applications-trends/. [Accessed 1 October 2017].

[7] Bechtel, "Transform your city with resilient smart infrastructure," Transform your city with resilient smart infrastructure, [Online]. Available: http://www.bechtel.com/smart-cities/. [Accessed 1 October 2017].

[8] N. Gagliordi, "Nvidia intros Metropolis video analytics platform for smart cities," 8 May 2017. [Online]. Available: http://www.zdnet.com/article/nvidia-intros-metropolis-video-analytics-platform-for-smart-cities/. [Accessed 1 October 2017].

[9] "#DataSmart News: Public Safety," 19 March 2017. [Online]. Available: http://datasmart.ash.harvard.edu/news/article/datasmart-news-public-safety-867. [Accessed 1 October 2017].

[10] System, AllGoVision Enhanced Monitoring: Surveillance, [Online]. Available: http://www.allgovision.com/enhanced-monitoring.php. [Accessed 1 October 2017].

[11] Bechtel, "How to transform your city with smart, resilient infrastructure," [Online]. Available: http://www.bechtel.com/getmedia/da33b7a3-663b-417c-8926-56f47136507d/Bechtel-How-to-transform-your-city-with-smart-resilient-infrastructure. [Accessed 1 October 2017].

[12] "A.I. Could Be a Firefighter's 'Guardian Angel'," [Online]. Available: https://www.jpl.nasa.gov/news/news.php?feature=6590. [Accessed 1 October 2017].

[13] Safe cities: Using smart tech for public security. [Online]. Available: http://www.bbc.com/future/bespoke/specials/connected-world/government.html. [Accessed 1 October 2017].

[14] "City of St. Albert Smart City Master Plan," 2016.

[15] Future of Privacy Forum, "Shedding Light on Smart City Privacy," [Online]. Available: https://fpf.org/2017/03/30/smart-cities/?utm_content=bufferb9445&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer. [Accessed 1 October 2017].

[16] Participatory Budgeting Network, "Online PB," [Online]. Available: https://pbnetwork.org.uk/category/themes/online-pb/. [Accessed 1 November 2017].

[17] S. Waldman and K. Kaminska, "Connecting emergency management organizations with digitally enabled emergent volunteering," Defence Research and Development Canada, Scientific Report, DRDC-RDDC-2015-R271, 2015.

[18] IBM, "Blockchain in Dubai: Smart cities from concept to reality.," 10 April 2017. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/04/blockchain-in-dubai-smart-cities-from-concept-to-reality/. [Accessed 1 November 2017].

[19] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., and Shen, X. S, Security and Privacy in Smart City Applications: Challenges and Solutions, University of Waterloo, 2016.

[20] Bartoli, A., Hernandez-Serrano, J., Soriano, M, Dohler, M., Kountouris, A. and Barthel, D., "Security and privacy in your smart city," [Online]. Available: http://smartcitiescouncil.com/sites/default/files/public_resources/Smart%20city%20security.pdf. [Accessed 1 October 2017].

[21] R. Kitchin, "Getting smarter about smart cities: Improving data privacy and data security," Department of the Taoiseach (on behalf of the Government Data Forum), 2016.

[22] C. Lévy-Bencheton and.E. Darra, "Cyber Security for Smart Cities: An Architecture Model for Public Transport," European Union Agency For Network And Information Security. December, 2015.

[23] A. Banafa, "A Secure Model of IoT with Blockchain," 21 December 2016. [Online]. Available: https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/?utm_source=views&utm_medium=article06&utm_campaign=MITcompany&utm_content=banafa-jan07. [Accessed 1 November 2017].

[24] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review,* vol. 154, no. 3, 2006.

[25] Ernst & Young, 2016., Cyber security: A necessary pillar of smart cities, Ernst & Young, 2016.

[26] "The Future of Smart Cities: Cyber-Physical Infrastructure Risk," U.S. Department of Homeland Security, 2015.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Smart Cities: Challenges and Opportunities for Public Safety and Security

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Tang, Helen; Waldman, Suzanne; Hubbard, Paul

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
January 2018	9	26

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Letter

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2018-L002	

11a. FUTURE DISTRIBUTION (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Any limitations on further dissemination of the document, other than those imposed by security classification.)

12. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

13. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Smart cities, community safety and security, community resilience, cyber-security