Smart Cities, Smart Bases and Secure Cloud Architecture for Resiliency by Design

AUTHORS
Lee W. McKnight, School of Information Studies, Syracuse University* & CSIAC Subject Matter Expert
Danielle Taana Smith, College of Arts and Sciences, Syracuse University
Patrick Prioletti, School of Information Studies, Syracuse University
Yusuf Abdul-Qadir, School of Information Studies, Syracuse University
Kevin Bornatsch, WiTec, School of Information Studies, Syracuse University

**Corresponding author: lmcknigh@syr.edu*

PREPARED BY:

Cyber Security & Information Systems Information Analysis Center

Operated by Quanterion Solutions Incorporated under contract FA8075-17-D-0001

266 Genesee Street
Utica, NY 13502

https://www.quanterion.com
qinfo@quanterion.com

Introduction

Smart cities critical infrastructure, economy, and governance is designed to sustainably improve the well-being of residents. (United States Government Accountability Office [GAO], 2019) Critical infrastructures such as energy, electricity grids, communications networks, transportation and water systems are digitally enhanced to provide smart services to city residents while ensuring security issues are well monitored and effectively addressed (GAO, 2019).

Smart Cities → Smart Bases

The smart city concept is readily applicable for military installations, and their neighboring communities, as military bases and cities may share residents, physical infrastructures, employment opportunities and the provision of a broad range of services. (Sharma & Raglin, 2019; CSIAC, 2020) This article illustrates how the smart city concept and especially regional secure cloud architectures can be applied in the military environment, and in mixed civilian – military contexts as well. (McKnight, 2020) For example, integrating a federated secure cloud architecture can lessen the risks of ransomware and other malicious cyber threats, and brings other benefits by increasing visibility for the base commander into all digital and cyberphysical systems operating on the base. (AFCEA, 2020; Lee, Bohn & Michel, NIST-SP 500-XXX, 2019) Of course, critical differences exist between cities and military bases. Military installations exist to train and house soldiers for peaceful and combat operations at home and in foreign countries. Bases also provide operational and logistical support for these missions. Because of their mission, military bases require a heightened level of cybersecurity; classified systems are beyond the scope of this article.

Cyberphysical 5G+ Security Risk Management for Smart Bases

Cyber threats are significant and all-encompassing threats to US national security. They target all American institutions, including federal, state, and local government, military, financial, healthcare, and educational institutions, and critical infrastructures. These threats are unrelenting.

A risk management approach to smart city/ smart base cybersecurity and privacy can assist military installations and their associated decision-makers and technology implementers as they consider, develop, implement, and/or operate Smart City capabilities and solutions. (McKnight 2020, NIST SCCF 2021) This approach engages stakeholders and begins the conversation around cybersecurity and privacy risk management. It verifies, supplements, and refines existing cybersecurity and privacy risk management processes. This approach can also identify key cybersecurity and privacy considerations that may be specific to smart base environments and solutions.

Smart Data Risk Classification Scheme

A smart data risk classification scheme can be applied to cities, counties, regions, states, nations, and bases. It assists both officials, service providers, the public and other stakeholders to recognize their shared responsibilities for smart city data security, privacy, ethics, and other rights (McKnight et al., 2019a).

1. **Red Data:** sensitive data including personally identifiable information - most controlled and restricted
2. **Yellow Data**: medium sensitivity information with possibly controlled access but by law can be shared more widely, although still with controls and monitoring
3. **Green Data**: low sensitivity data which can be shared openly - smart city civic and public data

An objective of a secure cloud architecture is to ensure that sensitive personal, corporate, and public service data are comprehensible and handled with safety. All users will be able to use the same simple cloud data classification language after reviewing these guidelines, allowing a unified approach to secure community cloud infrastructure. (McKnight 2019b, Underwood 2020)

Privacy and security challenges for smart cities, communities and bases are multi-faceted and complex. Lack of an overarching smart city cloud and privacy security architecture that articulates high level principles and practices which are plain and unambiguous to implement has contributed to the problem. The secure cloud architecture we present has a high likelihood of reducing the range of cyber-vulnerabilities that smart cities and their residents, and the public, community, and commercial firms confront. (McKnight, 2019a) A smart city architecture increases privacy, security, and rights-inclusive standards awareness by utilizing a simple cloud architecture that protects data and upholds privacy practices across sectors. Additionally, this framework lessens city operating costs and creates greater regional data transparency, which in turn increase service and product innovation. Implementation of the architecture can potentially contribute to a growth in commercial activities. (Kanowitz, 2019) With common cloud architecture guidelines ensuring smart community privacy, security, and data- rights are considered by design. (Goldstein, 2019) The economic benefits from emerging personal data revenue streams, new products, jobs, economic growth, and exports can contribute to growth of regional tax bases and positively serve energy, health, safety, and environmental objectives which include improvements in safety and quality of lives and widespread community acceptance, which will be replicated across the United States and adapted in other nations.

The vulnerabilities and threats experienced in many smart city environments are like those commonly found in the traditional enterprise information technology environment (Wong, 2019). As dependence on systems increase, there is a corresponding increase in the number of threats (Johnson et al., 2011). An overarching smart city cloud architecture is needed to provide guidelines on privacy and security, independent of industry or use case. (McKnight, 2019b) This framework aims to direct municipalities and other smart city implementation partners towards a secure and privacy-considerate smart city deployment. Risk is often calculated as a formula of Vulnerability (V) times Threat (T) times Consequence (C) (R = V x T x C) (Wong, 2019). Vulnerabilities are the weaknesses in a system; on their own, vulnerabilities are not a risk. A risk exists only when a threat that could misuse the vulnerability and a (negative) consequence are combined. Vulnerabilities can be eliminated by installing updates (e.g., patches) and altering configuration settings (Fagan et al., 2020).

Once risks are identified, it is important to assign a likelihood, impact, and overall rating to each risk. The overall rating is determined based on the likelihood and impact rating.

Table1. Three level data risk classification scheme

Green	Data that can be shared freely (i.e.: Open Data Lake, Civic Data Repository, Open Data Observatories, etc.)
Yellow	Data that can be shared with selected parties • Certain types of PII and other controlled information that may or may not be shared beyond an application with permission. • Some of this data could be shared with the permission of the individual from which the data was collected in return for compensation.
Red	Data that cannot be shared • Controlled proprietary information. • No automated sharing of data if not by a vetted and approved smart contract; sharing of data requires explicit approval.

(Source: McKnight 2019a)

The large amount of data and infrastructure has resulted in systems continually becoming more complex, and requiring clear and consistent security, in addition to privacy requirements and policies. Smart cities run largely on cloud services for efficiency and affordability reasons. (Kanowitz, 2019) Architecture guidelines and security policies help protect citizens' rights and ignite growth of smart city open data lakes, therefore encouraging civic engagement and data privacy security/rights-inclusive innovation, entrepreneurship, and economic development. Policy design and implementation are critical within the cloud architecture framework presented here to improve outcomes.

Each smart city deployment should create and distribute its own policies and procedures about all aspects of the smart city. Components that should be addressed in a dedicated policy/standards document include Data Security/Data Integrity, Information Security & Assurance, Identity and Access Management, Information Security Governance, Change Management and Business Continuity/Disaster Recovery.

The failure to proactively manage cybersecurity and privacy risks can be a detriment to smart city initiatives and can negatively impact the very systems intended to improve city services and citizens' livelihoods (McKnight, 2020). Implementation of this architecture can help to focus and prioritize resources on sensitive data in need of protection more efficiently. It also enables and encourages wide access to open government data so that researchers, students, non-profits, start-ups, and technology companies supporting the city and the public can participate and conduct their own analyses on civic data. Additionally, creating jobs while building more effective constituent services are among the objectives of many smart city projects. These guidelines suggest that jobs created are more likely to be sustainable and scalable if designed to work with NIST standards and best practice recommendations. (NIST SCCF, 2021)

Table 2. Risk matrix (likelihood x impact)

Likelihood	**Almost Certain**	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
	Likely	**Medium**	**Medium**	**High**	**High**	**Extreme**
	Possible	**Low**	**Medium**	**Medium**	**High**	**High**
	Unlikely	**Low**	**Low**	**Medium**	**Medium**	**High**
	Rare	**Low**	**Low**	**Low**	**Medium**	**High**
		Insignificant	**Minor**	**Moderate**	**Major**	**Critical**
		Impact				

Smart Base SARS2 Early Warning Wastewater Surveillance Platform

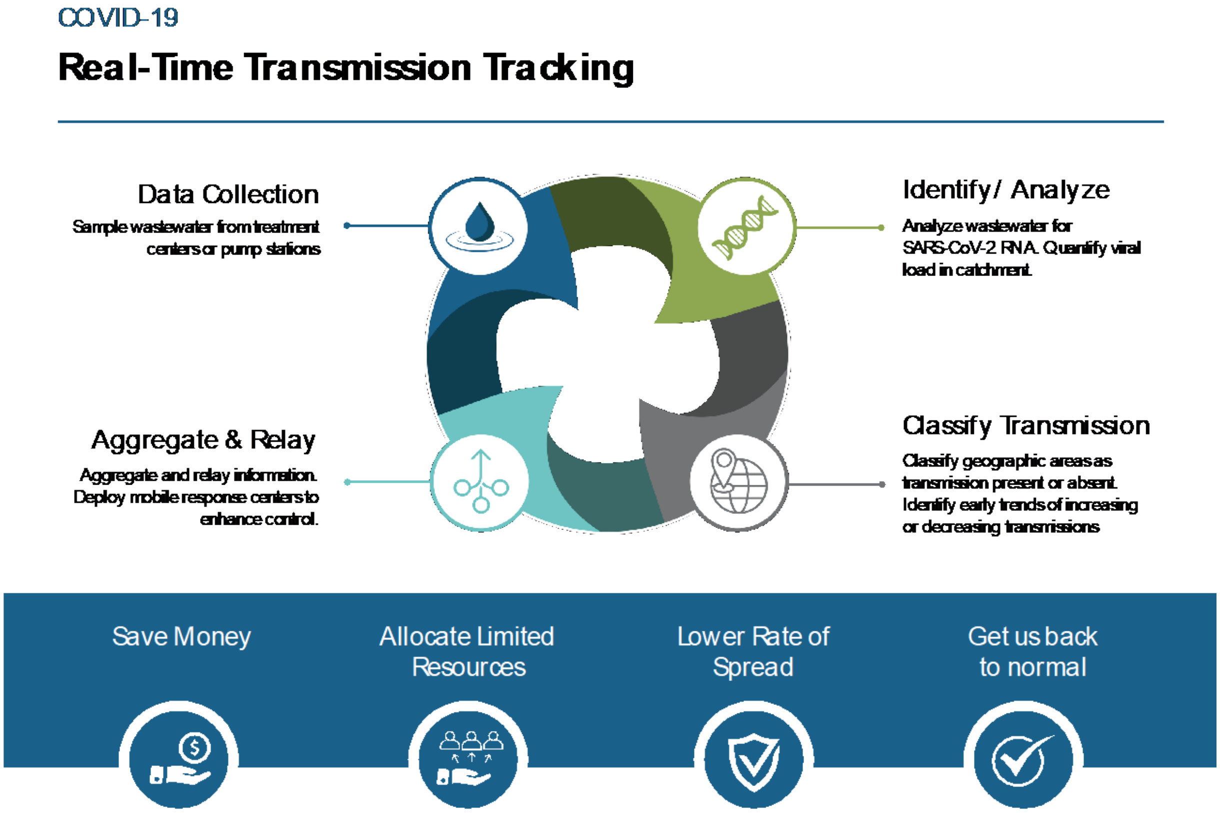
The SARS2 Early Warning Wastewater Surveillance Platform is a use case of implementation of the cloud privacy security rights-inclusive architecture during a global disaster. Goals of the Platform are to estimate SARS-CoV-2 transmission trends in real time, include provision of instant feedback on social distancing and reopening phases, predict hospitalizations from COVID-19 and provide confidence in the absence of transmission for areas with zero cases.

Severe Respiratory Acute Syndrome Corona Virus 2 (SARS COV2), part of the Corona Virus group, is the virus that causes CoVid-19 (National Institutes of Health, 2020). Disease is a nationally and globally destabilizing factor because it damages economic, social, political, and other infrastructures, and contributes to increased conflict within and between countries. Impacts of CoVid-19 include socio-economic and political disruption, impeded economic development, diversion of resources and a significant threat to national and international security.

Pandemic illness presents a particular challenge to the military's mission readiness and preparedness. During World War I, pandemic influenza and other infectious diseases caused more fatalities than combat and led to an estimated 8.7 million lost duty days among enlisted soldiers (Byerly, 2010). The impact of epidemic infectious disease on military readiness cannot be overstated, as infectious disease epidemics have frequently altered the course of military campaigns (Roy et al., 2018). With increasing numbers of novel infectious diseases emerging across the globe (Jones et al., 2008; Jappah & Smith, 2015), early warning of these threats, in the military context, is vitally important.

Wastewater monitoring can provide an early warning platform for SARS-CoV-2 infections, and for other diseases. First developed in the 1990s to track poliovirus circulation (Asghar et al., 2014; Brouwer et al., 2018), wastewater monitoring provides a non-invasive and cost-effective method of assessing pathogens circulating within a population. For patients with COVID-19, SARS-CoV-2 RNA is shed in human feces and other bodily fluids (Chen et al., 2020; Wang et al., 2020; Xu et al., 2020), and can be detected in wastewater (Medema et al., 2020; Green et al., 2020; Wu et al., 2020; Nemudryi et al., 2020). Importantly, increases in the levels of SARS-CoV-2 ribonucleic acid (RNA) in the wastewater provides 1 to 2 weeks' warning relative to increases in the number of COVID-19 cases in a health system (Wurtzer et al., 2020; Peccia et al., 2020). The SARS2 Early Warning Wastewater Surveillance Platform can be applied to military installations and their surrounding communities.

Next steps towards COVID-19 resilient smart bases include agreement on public-facing data, and matching case data with sewer sheds. These steps are necessary to inform interpretation of RNA in wastewater and to improve feedback loops. Public health surveillance authorization is necessary for ethics and approval by Institutional Review Boards. Military installations can partner with area firms and universities to accelerate adoption and innovation of this Platform.



COVID-19

Real-Time Transmission Tracking

Data Collection

Sample wastewater from treatment centers or pump stations

Identify/ Analyze

Analyze wastewater for SARS-CoV-2 RNA. Quantify viral load in catchment.

Aggregate & Relay

Aggregate and relay information. Deploy mobile response centers to enhance control.

Classify Transmission

Classify geographic areas as transmission present or absent. Identify early trends of increasing or decreasing transmissions

Save Money

Allocate Limited Resources

Lower Rate of Spread

Get us back to normal

(Source: Re-printed with permission: Larsen/Syracuse University 2019)

Conclusion: Lessons for Smart Cities and Bases

Smart cities and bases should always be vigilant, as both cyberphysical risks and opportunities are ubiquitous. Designing smart cities and bases is a growing challenge, in the face of growing cybersecurity threats. Distributed interests throughout smart cities/communities and bases make progress and coordination difficult, and ad-hoc and hard-to-define architectures and networks continue to challenge cybersecurity. Inherent advantages of attackers include choice of time and place and illicit actors incentivized to strengthen crime industry and grow revenue. The pattern is the same, although the tools – early DDoS, macro viruses, emerging APT, escalating DDoS, Botnets, Ransomware, etc. – are different. Yet, a smart city framework that is not smart by design remains a poor alternative.

Smart base innovators can leverage ISPs/MSPs and set up win/win conditions. They can utilize partnership red teams. Financial and cyberphysical risk analyses are also critical. Innovators must check all enterprise software and user apps to safeguard against software and systems risks. This includes insistence on documentation, cyber-physical risk management and continuous improvement. All workforce should be trained, and a focus should be placed on growing local expertise. And finally, think Red Yellow Green Data!!!

While smart city initiatives offer unprecedented opportunities to enhance the well-being of millions of community residents, their implementation may not necessarily result in benefits for all citizens. As such, these initiatives should be deliberately designed, implemented, and monitored to improve the population well-being of all citizens (OECD, 2020). This framework requires smart governance and multi-sectoral cooperation that aligns with "local and national strategic priorities and that embraces efficiency, effectiveness and sustainability dimensions (OECD, 2020).

With adaptation of the secure cloud framework, the military can continue to make progress in becoming a smart military. This adaptation adds value as the US military works to achieve its operational mission of a smart military. This framework can help in enhancing military operations and meeting emerging challenges of the 21st century.

References

[1] Asghar, H., Diop, O.M., Weldegebriel, G., Malik, F., Shetty, S., El Bassioni, L., Akande, A.O., Al Maamoun, E., Zaidi, S., Adenjii, A.A., Burns, C.C, Deshpande, J., Oberste, M.S., & Lowther, S.A. (2014). Environmental surveillance for polioviruses in the global polio eradication initiative*. J. Infect. Dis*. 210, S294–S303.

[2] Brouwer, A.F., Eisenberg, J.N.S., Pomeroy, C.D., Shulman, L.M., Hindiyeh, M., Manor, Y., Grotto, I., Koopman, J.S., & Eisenberg, M.C. (2018). Epidemiology of the silent polio outbreak in Rahat, Israel, based on modeling of environmental surveillance data. *Proc. Natl. Acad. Sci. U. S. A.* 115, E10625–E10633.

[3] Byerly, C. (2010). The U.S. military and the influenza pandemic of 1918-1919. *Public Health Rep.* 125, pp. 82–91.

[4] Chen, Y., Chen, L., Deng, Q., Zhang, G., Wu, K., Ni, L., Yang, Y., Lui, B., Wang, W., Wei, C., Yang, J., Ye, G., & Cheng, Z. (2020). The presence of SARS-CoV-2 RNA in the feces of COVID-19 patients. *J. Med. Virol.* 92, pp. 833–840.

[5] Fagan, M., Megas, K.N., Scarfone, K., & Smith, M. (2020). Recommendations for IoT device manufacturers: Foundational activities and core device cybersecurity capability baseline," *National Institute of Standards and Technology.*

[6] Goldstein, P. (2019) 'How a Secure Cloud Architecture Helps Smart Cities,' *StateTech,* https://statetechmagazine.com/article/2019/08/how-secure-cloud-architecture-can-help-smart-cities

[7] Green, H., Wilder, M., Middleton, F.A., Collins, M., Fenty, A., Gentile, K., Kmush, B., Zeng, T., & Larsen, D.A. (2020). Quantification of SARS-CoV-2 and cross-assembly phage (crAssphage) from wastewater to monitor coronavirus transmission within communities, *medRxiv*, preprint, 2020. DOI: 10.1101/2020.05.21.20109181

[8] Jappah, V., & Smith, D. (2015). Global governmentality: Biosecurity in the era of infectious diseases. *Global Public Health.* 10(10), pp. 1139-1156.

[9] Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2011). Guide for security-focused configuration management of information systems. *National Institute of Standards and Technology.*

[10] Jones, K.E., Patel, N.G., Levy, M.A., Storeygard, A., Balk, D., Gittleman, J.L., & Daszak, P. (2008). Global trends in emerging infectious diseases. *Nature* 451, pp. 990–993.

[11] Kanowitz, S., (2019) A Secure Cloud Architecture for Smart Cities, *GCN*, https://gcn.com/articles/2019/07/11/smart-city-secure-cloud-architecture.aspx

[12] Lee, C, Bohn, R. & Michel, M. (2019) The Cloud Federation Reference Architecture, NIST SP-500-XXXX. https://doi.org/10.6028/NIST.SP.XXXX

[13] McKnight, L.W., Abdul-Qadir, Y., Prioletti, P., Smith, D.T., Bornatsch, K., (2020). 'Smart City and Community Data Risk Management with Secure Cloud Architecture,' Proceedings of the 18th IEEE International Smart City Conference, IEEE Xplore (in press).

[14] McKnight, L.W., Bornatsch, K., Abdul-Qadir, Y., Edelstein, S., & Jensen, L. (2019a). Towards a smart city cloud privacy, security, and rights-inclusive architecture. SC3-cpSRIA Action Cluster Blueprint v0.8, *Global City Teams Challenge*.

[15] McKnight, L.W., Bornatsch, K., Abdul-Qadir, Y., Edelstein, S., & Jensen, L. (2019b). Secure cloud architecture. GCTC SC3 cpSria, 2019. https://gctc.opencommons.org/images/f/ff/CommunityCloudPrivacy.pdf

[16] Medema, G., Heijnen, L., Elsinga, G., Italiaander, R., & Brouwer, A. (2020). Presence of SARS- Coronavirus-2 in sewage. *Environmental Science & Technology Letters,* 7, 7, pp. 511-516. doi: 10.1021/acs.estlett.0c00357

[17] National Institutes of Health. (2020). SARS-CoV-2 stability like original SARS virus. *US* Department of Health and Human Services. https://www.nih.gov/news-events/news-releases/new-coronavirus-stable-hours-surfaces

[18] National Institute of Standards and Technology (NIST). (2014). Cyber security framework (CSF). https://www.nist.gov/cyberframework

[19] National Institute of Standards and Technology (NIST). (2018). Special Publication (SP) 800-37 Revision 2, *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy.* https://csrc.nist.gov/News/2018/rmf-update-nist-publishes-sp-800-37-rev-2

[20] National Institute of Standards and Technology, (NIST). (2021). Smart City and Community Framework Series. *Smart City and Community Security and Privacy Risk Management Framework* (in press).

[21] Nemudryi, A., Nemudraia, A., Surya, K., Wiegand, T., Buyukyoruk, M., Wilkinson, R., & Wiedenheft, B. (2020). Temporal detection and phylogenetic assessment of SARS-CoV-2 in municipal wastewater. *medRxiv*. doi:10.31857/s0023476120020216

[22] Organization for Economic Co-operation and Development (OECD). (2020). Smart cities and inclusive growth: Building on the outcomes of the 1st OECD roundtable on smart cities and inclusive growth. https://www.oecd.org/cfe/cities/OECD_Policy_Paper_Smart_Cities_and_Inclusive_Growth.pdf

[23] Peccia, J., Zulli, A., Brackney, D.E., Grubaugh, N.D., Kaplan, E.H., Casanovas-Massana, A., Ko, A.I., Malik, A.A., Wang, D., Wang, M., Warren, J.L., Weinberger, D.M., & Omer, S.B. (2020). SARS-CoV-2 RNA concentrations in primary municipal sewage sludge as a leading indicator of COVID-19 outbreak dynamics. *medRxiv,* 2020.05.19.20105999; doi: https://doi.org/10.1101/2020.05.19.20105999

[24] Roy, K., & Ray, S. (2018). War and epidemics: A chronicle of infectious diseases. *J. Mar. Med. Soc.* 20, pp. 50–54.

[25] Sharma, P.K., & Raglin, A. (2019). “IoT in Smart Cities: Exploring Information Theoretic and Deep Learning Models to Improve Parking Solutions,” *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*

[26] Underwood, K., Cloud Architecture Offers Security to Cities, *AFCEA SIGNALS*, May 1, 2020 https://www.afcea.org/content/cloud-architecture-offers-security-cities

[27] United States Central Intelligence Agency. (2017). WikiLeaks Task Force: Final report. Homeland Security Digital Library. https://www.hsdl.org/?view&did=840216

[28] United States Congress. (2016). Executive summary of review of the unauthorized disclosures of former National Security Agency contractor Edward Snowden. House Permanent Select Committee on Intelligence: http://intelligence.house.gov/

[29] United States Government Accountability Office. (2019). Cybersecurity challenges facing the nation – High risk issue. https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary

[30] Wang, W., Xu, Y., Gao, R., Lu, R., Han, K., Wu, G., & Tan, W. (2020). Detection of SARS-CoV-2 in Different Types of Clinical Specimens. *JAMA - J. Am. Med. Assoc*. 323, pp. 1843–1844.

[31] Wong, P. (2019). Global city teams challenge 2019: Smart secure cities and communities challenge (S3). In *GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook - 2019.*

[32] Wu, F., Xiao, A., Zhang, J., Gu, X., Lee, W.L., Kauffman, K., Hanage, W., Matus, M., Ghaeli, N., Endo, N., Duvallet, C., Moniz, K., Erickson, T., Chai, P., Thompson, J., & Alm, E. (2020). SARS-CoV-2 titers in wastewater are higher than expected from clinically confirmed cases. *medRxiv.* doi: https://doi.org/10.1101/2020.04.05.20051540

[33] Wurtzer, S., Marechal, V., Mouchel, J.M., Maday, Y., Teyssou, R., Richard, E., Almayrac, J.L., & Moulin, L. (2020). Evaluation of lockdown impact on SARS-CoV-2 dynamics through viral genome quantification in Paris wastewaters. *medRxiv.* doi: https://doi.org/10.1101/2020.04.12.20062679

[34] Xu, Y., Li, X., Zhu, B., Liang, H., Fang, C., Gong, Y., Guo, Q., Sun, X., Zhao, D., Shen, J., Zhang, H., Liu, H., Xia, H., Tang, J., Zhang, K., & Gong, S. (2020). Characteristics of pediatric SARS-CoV-2 infection and potential evidence for persistent fecal viral shedding. *Nat. Med*. 26, pp. 502–505.

[35] Zola, A., (2019) How to Secure Data in Smart Cities, Intersog Blog https://intersog.com/blog/how-to-secure-data-in-smart-cities/