UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

The Cybersecurity Risks of Smart City Technologies

What Do The Experts Think?

KAREN TRAPENBERG FRICK, GISELLE MENDONÇA ABREU,
NATHAN MALKIN, ALEXANDRA PAN, ALISON E. POST

CLTC WHITE PAPER SERIES

The Cybersecurity Risks of Smart City Technologies

What Do The Experts Think?

KAREN TRAPENBERG FRICK, GISELLE MENDONÇA ABREU,
NATHAN MALKIN, ALEXANDRA PAN, ALISON E. POST

FEBRUARY 2021

CENTER FOR LONG-TERM CYBERSECURITY

University of California, Berkeley

Acknowledgments

We would like to acknowledge the following organizations and individuals who assisted us in some way with this report. The staff at the Center for Long-Term Cybersecurity provided helpful advice and assistance with distributing our survey. The RSA, HackerOne, the Information Systems Audit and Control Association, the International Information System Security Certification Consortium, the Meeting of the Minds, Joint Venture Silicon Valley, Plug and Play, and the National Strategic Planning and Analysis Research Center kindly helped us to reach cybersecurity experts. We also thank Camille Crittenden, Chappell Lawson, Kenichi Soga, and Brian de Vallance for their advice and help with establishing contacts in the cybersecurity community.

Contents

Executive Summary

Local officials receive a barrage of information about "smart city" solutions to long-standing problems, such as traffic congestion, crime, inefficient use of power and water, and detecting leaky pipes. Which of these myriad technological solutions hyped by consultancies, conferences, and vendors are worth considering? And how should local governments consider the countervailing risks of cyberattack that such new systems may introduce?

In this report, we aim to help local-level policymakers better understand how cyber-risks vary among different smart city technologies. We present the results from a 2020 survey in which 76 cybersecurity experts ranked different technologies according to underlying technical vulnerabilities, their attractiveness to potential attackers, and the potential impact of a successful serious cyberattack.

According to our survey, not all smart city technologies pose equal risks. Cybersecurity experts judged emergency alerts, street video surveillance, and smart traffic signals to be riskier than other technologies in our study. Local officials should therefore consider whether cyber-risks outweigh the potential gains of technology adoption on a case-by-case basis, and exercise particular caution when technologies are both vulnerable in technical terms *and* constitute attractive targets to capable potential attackers because the impacts of an attack are likely to be great.

Introduction

The term "smart city" is generally used to describe the deployment of information and communication technologies (ICT) to improve urban services and infrastructure. Media and conference coverage suggest smart city technologies are all the rage, and investment in smart city technologies is expected to reach $327 billion by 2025 (from $96 billion in 2019), according to research by consulting firm Frost & Sullivan.[1] Technologies such as open data portals and online broadcasting of public meetings are lauded as means of increasing the transparency of government operations, while online complaint registries and public comment solicitations are touted as vehicles for increasing citizen participation. Other technologies promise to improve the sustainability or cost-effectiveness of service delivery. Smart meters for electricity and water customers, for example, can help citizens and utilities manage scarce water and energy resources more effectively.

Critics of smart city technologies point to potential threats posed when local jurisdictions adopt these digital systems. One key concern is cybersecurity. Critics argue that introducing new technologies that increase the connectedness of service delivery systems and government operations with the internet can expose local communities to cyberattacks by a variety of malicious actors. Cyberattacks could generate significant damage, including the shut-down or compromising of vital services such as electricity or water. In numerous cases, ransomware attacks have even locked city staff from municipal computers and networks, bringing operations to a halt until large payments are made.[2] Cyberattacks could also lead to the capture and misuse of citizens' sensitive personal information or video footage of their activities. In January 2021, a cyberattack even allowed an outsider to temporarily alter chemical concentrations in a local water supply system.[3] Concerns about such threats have prompted the Department of Homeland Security to establish a program to address the cybersecurity of "critical infrastructure" like transportation and water systems.

Do all smart city technologies pose equivalent cybersecurity risks? In this report, we aim to help local-level policymakers trying to decide whether or not to adopt particular technologies

1 Valente, Francesca. "Smart Cities to Create Business Opportunities Worth $2.46 Trillion by 2025, says Frost & Sullivan," Frost & Sullivan Media Release, Oct 29, 2020, https://ww2.frost.com/news/press-releases/smart-cities-to-create-business-opportunities-worth-2-46-trillion-by-2025-says-frost-sullivan/.

2 Teale, Chris. "Ransomware attacks 'raising the bar' as cities struggle to respond," Smart Cities Dive, August 27, 2020, https://www.smartcitiesdive.com/news/ransomware-attacks-smart-cities-response/584202/.

3 Robles, Frances and Perlroth, Nicole. "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town," New York Times, February 8, 2021, https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.

by examining how their relative cyber-risks may vary. We present the results from a 2020 survey in which 76 cybersecurity experts ranked different technologies according to underlying technical vulnerabilities, their attractiveness to potential attackers, and the potential impact of a successful serious cyberattack.

Our survey results indicate that smart city technologies vary considerably in terms of the level of risks posed, with certain technologies—such as emergency alerts, street video surveillance, and smart traffic signals—posing greater risks in aggregate than others. Local officials should therefore consider whether cyber-risks outweigh the potential gains of technology adoption on a case-by-case basis, and exercise particular caution when technologies are both vulnerable in technical terms *and* constitute attractive targets to capable potential attackers because the impacts of an attack are likely to be great.

Comparing Cybersecurity Risks Across Technologies

Comparing the respective risks of cyberattacks across technologies requires considering not only the technology itself. It also requires attention to the interests and capabilities of those who may carry out attacks, and the potential impact of successful attacks if they do occur. In this study, we build on existing scholarship in cybersecurity to develop a framework for assessing the relative risks posed by different technologies (see Table 1).

TABLE 1. CYBERSECURITY RISK ASSESSMENT FRAMEWORK FOR "SMART CITY" TECHNOLOGIES

DOES THE UNDERLYING TECHNOLOGY POSSESS IMPORTANT CYBER VULNERABILITIES?
• How large is the "attack surface," the number of possible points of entry for an attack? • How complex is the technology, and how many interdependencies exist between systems?
WHAT SORT OF CONSEQUENCES WOULD A SUCCESSFUL CYBERATTACK HAVE?
• Would service disruptions occur? How consequential would such disruptions be? Would service disruptions affect other systems or services? • Would personal data be compromised? What sort of data, and at what scale? What would be the impacts on public trust? On local agency finances?
WOULD A CAPABLE ORGANIZATION BE LIKELY TO EXECUTE AN EFFECTIVE CYBERATTACK ON THIS TECHNOLOGY?
• Which potential attackers are likely to be most effective? • Are these potential attackers interested in the technology in question?

Posing these questions is a useful exercise when considering the adoption of new technologies; it encourages one to break down cybersecurity risk into different components. Some technologies that may be vulnerable in technical terms may not be of interest to threat actors, for example. Other technologies may be less vulnerable, but may be attractive enough to incentivize attackers to find vulnerabilities; if successful attacks on these technologies would have catastrophic consequences, public agencies should be wary.

Note that this approach does not capture additional, important sources of variation in cybersecurity. It fails to capture differences in the level of cyber-protections adopted by public agencies to guard against attacks, including firewalls, regular security updates, etc. It also fails to capture differences in the training and behavior of personnel who are using the technology. We return to these issues below.

Study Design

We administered our online survey of cybersecurity experts during the summer and fall of 2020. In the survey, we asked respondents to characterize the cybersecurity risks posed by nine different smart city technologies from the water, transportation, and security sectors (see Table 2). Following existing scholarship on cybersecurity, we chose technologies that vary in terms of their technical complexity and the size of the "attack surface"—i.e., the number of potential entry points for cyberattacks—within each policy area.

TABLE 2. SMART CITY TECHNOLOGIES INCLUDED IN SURVEY

SECTOR	TECHNOLOGY
WATER AND SANITATION	• Smart Waste/ Recycling Bins
	• Satellite Water Leak Detection
	• Water Consumption Tracking ("Smart Meters")
TRANSPORTATION	• Smart Tolling
	• Smart Traffic Lights/Signals
	• Public Transit Open Data (e.g. GTFS feeds)
SECURITY/POLICING	• Emergency or Security Alerts
	• Gunshot Detection
	• Street Video Surveillance

Experts were posed a series of questions about different contributors to cyber-risks. They were asked to rank each technology according to how easy it would be for an adversary to discover and carry out an attack, and the potential impact if a successful attack occurred. They were also asked to rank the relative effectiveness of different actors that could carry out cyberattacks, and to select the technologies such actors would be most interested in targeting. Prior to answering these questions, experts were asked to characterize their level of familiarity with the different technologies. We did not ask respondents to rank technologies with which they indicated they were unfamiliar, thereby ensuring that respondent rankings would be based upon adequate knowledge.

Cybersecurity experts were recruited to complete our survey through professional and conference organizations common in this field (see Table 3). We also publicized the survey through the social media accounts of the Center for Long-Term Cybersecurity, prominent

cybersecurity credentialing organizations (ISACA and ISC2), and influential cybersecurity experts. We recruited 76 respondents through these various avenues. Respondents' self-reported professional activities and level of familiarity with the smart city technologies suggested that our recruitment strategy succeeded in attracting cybersecurity professionals: 76% of our respondents reported that their jobs involved cybersecurity. Fifty percent of respondents worked primarily in the private sector, 54% of respondents were 55 years or older, and 64% identified as male.

TABLE 3: SURVEYED EXPERTS BY RECRUITMENT CHANNEL

RECRUITMENT CHANNEL/ORGANIZATION	NUMBER OF RESPONSES
Adaptable Security Cybersecurity Symposium for Smart Cities (conference)	13
SCADA and Control Systems Security Group (online professional group forum)	12
Twitter	12
Miscellaneous outreach (newsletter of the UC Berkeley Center for Long-Term Cybersecurity, RSA conference newsletter, HackerOne conference newsletter)	11
Symposium on Usable Privacy and Security Conference (conference)	6
Information Systems Audit and Control Association (ISACA) (professional organization)	5
Meeting of the Minds (non-profit group)	4
Informal distribution among hackers through university contact	4
American Public Transportation Association cybersecurity member group	2
East Bay Municipal Utility District IT department employees	2
International Information System Security Certification Consortium (certification body)	2
American Society of Civil Engineers (ASCE) Emerging Technologies Committee	2
National Strategic Planning and Analysis Research Center (academic research center)	1

Survey Findings

Cybersecurity experts indicated that some smart city technologies present greater risks than others. These differences can be attributed to the fact that those technologies perceived as more vulnerable in technical terms are also most likely to generate the largest impacts in the event of a successful attack, and to attract the attention of effective threat actors.

The experts' rankings of the underlying technical vulnerability of the nine technologies indicated that smart waste and recycling bins and satellite water leakage systems are perceived to be less vulnerable than the other technologies (e.g., emergency or security alerts, video surveillance systems, smart traffic lights).[4] Emergency and security alerts were perceived as most vulnerable and satellite leak detection were ranked as least vulnerable in technical terms[5] (see Table 4); when respondents indicated they had little familiarity with specific technologies, we did not utilize their responses to calculate these rankings.

TABLE 4. EXPERT ASSESSMENTS OF CYBERSECURITY OF SMART CITY TECHNOLOGIES

	RANKING: TECHNICAL VULNERABILITY	RANKING: IMPACT OF A SUCCESSFUL ATTACK	RANKING: INTEREST LEVEL OF NATION-STATE ATTACKERS**
Emergency and Security Alert Systems	1	1	1
Street Video Surveillance	2	3	2
Smart Traffic Lights/Signals	3	2	3
Water Consumption Tracking	4	6	5
Smart Tolling	5	7	8*
Public Transit Open Data	6	5	4
Gunshot Detection	7	4	8*
Smart Waste or Recycling Bins	8	9	9
Satellite Water Leak Detection	9	8	6

*Smart tolling and gunshot detection tied for 8th place.

**Nation-States are included here as they were ranked as the most effective threat actor, along with insiders

4 We assessed the statistical significance of differences between the rankings of different pairs of technologies using Dunn's test, a method of testing for differences in pairwise comparisons which can accommodate incomplete ranking data and tied ranks.

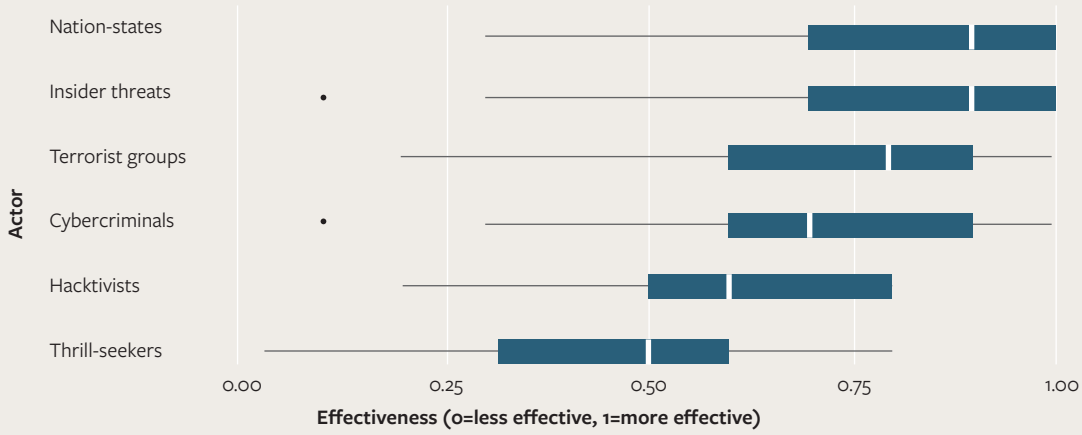
5 Overall rankings were calculated using a Markov method. The Markov method constructs a ranking based on head-to-head comparisons between each ranked object, with lower-ranked objects casting "votes" for higher-ranked objects.

Importantly, the technologies perceived by respondents as most vulnerable to cyberattacks also ranked as most likely to generate *significant impacts* in the event of a successful attack (Table 4). Emergency and security alert systems, street video surveillance, and smart traffic lights were ranked as significantly *more* vulnerable to cyberattacks; moreover, cyberattacks on these technologies were viewed as likely to generate a significantly *higher* impact if successful ($p < 0.01$). In contrast, smart waste or recycling bins and satellite water leak detection were ranked as significantly *less* vulnerable and *lower* impact compared to other technologies ($p < 0.01$).[6]

Written responses to our open-ended questions indicated the types of attack scenarios envisioned by the surveyed experts. Eighteen of the 76 respondents explained that tampering with traffic lights could cause accidents and gridlock, and prevent emergency vehicles from reaching their destinations. Ten of the 76 respondents described how spoofed emergency alerts could cause widespread panic and civil unrest.

Surveyed experts indicated that nation-states and insiders would be most effective at executing cyberattacks, compared with thrill seekers, cybercriminals, terrorist groups, and hacktivists. Responses to our open-ended questions indicate that the experts consider nation-states to possess strong motives for attacks on infrastructure, and to be able to mobilize the significant

FIGURE 1. EXPERT PERCEPTIONS OF THE EFFICACY OF DIFFERENT CYBER THREAT ACTORS



6 Markov ranking methods were used for this survey question as well, and the Dunn's test was similarly used to test for statistical significance of differences between specific pairs of technologies.

resources needed to launch attacks from the outside. Insiders, meanwhile, have easy access and the skills and knowledge to carry out effective attacks. Crucially, the surveyed experts indicated that the three technologies ranked as most vulnerable and impactful would be of greatest interest to nation-states: emergency or security alerts, street video surveillance, and smart traffic lights or signals.

The composite picture that emerges from these experts' rankings suggests that, among the technologies included in our study, those that are most vulnerable in technical terms are also most likely to be targeted by nation-state attackers. Moreover, such attacks are likely to generate strong impacts.

Conclusion

Our survey results indicate that smart city technologies are not created equally when it comes to cyber-risk. Cybersecurity experts judged emergency and security alerts, smart traffic signals, and video surveillance to be much riskier than many others. Several key factors contribute to this variation: a) varying levels of technical vulnerability; b) differing levels of interest in attacks by those best positioned to execute successful cyberattacks; and c) differing levels of disruption caused by attacks. Cybersecurity professionals typically focus on these factors when considering whether or not a particular technology is vulnerable; local officials should do the same.

Fortunately, the number of resources available for local agencies interested in understanding the potential risks of different technologies is increasing: the Department of Homeland Security offers training programs for local officers,[7] academic institutions like MIT offer online courses and certification programs focused specifically on the cybersecurity of smart city technologies,[8] and membership organizations like the American Waterworks Association[9] and the Technology Approval Group (TAG)[10] run committees or meetings that examine the cybersecurity risks of specific smart city technologies. We encourage local public agencies to make use of these and similar resources when making assessments of the cybersecurity risks posed by particular technologies.

It is important to stress that factors beyond those examined in our survey contribute to cyber-risks. As mentioned above, local cybersecurity efforts and programming, cybersecurity training, and regular system maintenance can help guard any system against attacks. Vendors offering smart city technologies will also vary in the extent to which they include strong cybersecurity protections. In addition, our study only includes a subset of the smart city technologies that local agencies may be considering. Our sample of experts was relatively small and the respondents had differing levels of familiarity with the technologies considered; the perceptions of the experts may not be representative of those of the cybersecurity expert community more broadly.

7 Cybersecurity & Infrastructure Security Agency (CISA), "Infrastructure Security," https://www.cisa.gov/infrastructure-security.

8 "Cybersecurity: A Social Engineering Approach at MIT: Teaching, Research, and City-Based Practice," https://urbancyberdefense.mit.edu/CybersecurityClinic.

9 American Water Works Association (AWWA), "AWWA Resources on Cybersecurity," https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance.

10 The Technology Approval Group (TAG), https://www.isleutilities.com/services/technology-approval-group/tag-us.

Still, experts' responses point to significant variation in the cybersecurity of smart city technologies that should be kept in mind by local policymakers when considering new purchases. Rather than embracing new technologies as quickly as possible, or rejecting new tools across the board due to cybersecurity concerns, city officials should weigh the costs and benefits on a case-by-case basis. In some cases, the potential gains in terms of lives saved may be so significant that they outweigh security risks; this may, in fact, be the case for emergency and security alerts. In other cases, cyber-risks may outweigh potential benefits.

About the Authors

KAREN TRAPENBERG FRICK is Associate Professor in the Department of City and Regional Planning at UC Berkeley.

GISELLE MENDONÇA ABREU is a PhD Candidate in the Department of City and Regional Planning at UC Berkeley.

NATHAN MALKIN is a PhD Candidate in the Department of Electrical Engineering and Computer Sciences at UC Berkeley.

ALEXANDRA PAN is a PhD Student in Civil and Environmental Engineering at UC Berkeley.

ALISON E. POST is Associate Professor of Political Science and Global Metropolitan Studies at UC Berkeley.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley